
# Amazon Web Services: Risk and Compliance

***December 2014***

(Consult http://aws.amazon.com/compliance/aws-whitepapers/

for the latest version of this paper)

This document is intended to provide information to assist AWS customers with integrating AWS into their existing control framework supporting their IT environment. This document includes a basic approach to evaluating AWS controls and provides information to assist customers with integrating control environments. This document also addresses AWS-specific information around general cloud computing compliance questions.

# Table of Contents

# Risk and Compliance Overview

Since AWS and its customers share control over the IT environment, both parties have responsibility for managing the IT environment. AWS's part in this shared responsibility includes providing its services on a highly secure and controlled platform and providing a wide array of security features customers can use. The customers' responsibility includes configuring their IT environments in a secure and controlled manner for their purposes. While customers don't communicate their use and configurations to AWS, AWS does communicate its security and control environment relevant to customers. AWS does this by doing the following:

- Obtaining industry certifications and independent third party attestations described in this document
- Publishing information about the AWS security and control practices in whitepapers and web site content
- Providing certificates, reports, and other documentation directly to AWS customers under NDA (as required)

For a more detailed description of AWS security please see the AWS Security Center. The AWS Overview of Security Processes Whitepaper covers AWS's general security controls and service-specific security.

## Shared Responsibility Environment

Moving IT infrastructure to AWS services creates a model of shared responsibility between the customer and AWS. This shared model can help relieve customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. It is possible for customers to enhance security and/or meet their more stringent compliance requirements by leveraging technology such as host based firewalls, host based intrusion detection/prevention, encryption and key management. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment of solutions that meet industry-specific certification requirements.

This customer/AWS shared responsibility model also extends to IT controls. Just as the responsibility to operate the IT environment is shared between AWS and its customers, so is the management, operation and verification of IT controls shared. AWS can help relieve customer burden of operating controls by managing those controls associated with the physical infrastructure deployed in the AWS environment that may previously have been managed by the customer. As every customer is deployed differently in AWS, customers can take advantage of shifting management of certain IT controls to AWS which results in a (new) distributed control environment. Customers can then use the AWS control and compliance documentation available to them (described in the AWS Certifications and Third-party Attestations section of this document) to perform their control evaluation and verification procedures as required.

The next section provides an approach on how AWS customers can evaluate and validate their distributed control environment effectively.

## Strong Compliance Governance

As always, AWS customers are required to continue to maintain adequate governance over the entire IT control environment regardless of how IT is deployed. Leading practices include an understanding of required compliance objectives and requirements (from relevant sources), establishment of a control environment that meets those objectives and requirements, an understanding of the validation required based on the organization's risk tolerance, and

verification of the operating effectiveness of their control environment. Deployment in the AWS cloud gives enterprises different options to apply various types of controls and various verification methods.

Strong customer compliance and governance might include the following basic approach:

1. Review information available from AWS together with other information to understand as much of the entire IT environment as possible, and then document all compliance requirements.
2. Design and implement control objectives to meet the enterprise compliance requirements.
3. Identify and document controls owned by outside parties.
4. Verify that all control objectives are met and all key controls are designed and operating effectively.

Approaching compliance governance in this manner will help companies gain a better understanding of their control environment and will help clearly delineate the verification activities to be performed.

# Evaluating and Integrating AWS Controls

AWS provides a wide range of information regarding its IT control environment to customers through white papers, reports, certifications, and other third-party attestations. This documentation assists customers in understanding the controls in place relevant to the AWS services they use and how those controls have been validated. This information also assists customers in their efforts to account for and to validate that controls in their extended IT environment are operating effectively.

Traditionally, the design and operating effectiveness of control objectives and controls are validated by internal and/or external auditors via process walkthroughs and evidence evaluation. Direct observation/verification—by the customer or customer's external auditor—is generally performed to validate controls. In the case where service providers, such as AWS, are used, companies request and evaluate third-party attestations and certifications in order to gain reasonable assurance of the design and operating effectiveness of control objective and controls. As a result, although customer's key controls may be managed by AWS, the control environment can still be a unified framework where all controls are accounted for and are verified as operating effectively. Third-party attestations and certifications of AWS can not only provide a higher level of validation of the control environment, but may relieve customers of the requirement to perform certain validation work themselves for their IT environment in the AWS cloud.

## AWS IT Control Information

AWS provides IT control information to customers in the following two ways:

1. **Specific control definition.** AWS customers are able to identify key controls managed by AWS. Key controls are critical to the customer's control environment and require an external attestation of the operating effectiveness of these key controls in order to comply with compliance requirements—such as the annual financial audit. For this purpose, AWS publishes a wide range of specific IT controls in its Service Organization Controls 1 (SOC 1) Type II report. The SOC 1 report, formerly the Statement on Auditing Standards (SAS) No. 70, Service Organizations report and commonly referred to as the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) report, is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). The SOC 1 audit is an in-depth audit of both the design and operating effectiveness of AWS's defined control objectives and control activities (which include control objectives and control activities over the part of the infrastructure AWS manages). "Type II" refers to the fact that each of the controls described in the report are not only evaluated for adequacy of design, but are also tested for operating effectiveness by

the external auditor. Because of the independence and competence of AWS's external auditor, controls identified in the report should provide customers with a high level of confidence in AWS's control environment. AWS's controls can be considered designed and operating effectively for many compliance purposes, including Sarbanes-Oxley (SOX) Section 404 financial statement audits. Leveraging SOC 1 Type II reports is also generally permitted by other external certifying bodies (e.g., ISO 27001 auditors may request a SOC 1 Type II report in order to complete their evaluations for customers).

Other specific control activities relate to AWS's Payment Card Industry (PCI) and Federal Information Security Management Act (FISMA) compliance. As discussed below, AWS is compliant with FISMA Moderate standards and with the PCI Data Security Standard. These PCI and FISMA standards are very prescriptive and require independent validation that AWS adheres to the published standard.

2. **General control standard compliance.** If an AWS customer requires a broad set of control objectives to be met, evaluation of AWS's industry certifications may be performed. With the AWS ISO 27001 certification, AWS complies with a broad, comprehensive security standard and follows best practices in maintaining a secure environment. With the PCI Data Security Standard (PCI DSS), AWS complies with a set of controls important to companies that handle credit card information. With AWS's compliance with the FISMA standards, AWS complies with a wide range of specific controls required by US government agencies. Compliance with these general standards provides customers with in-depth information on the comprehensive nature of the controls and security processes in place and can be considered when managing compliance.

AWS reports, certifications and third party attestations are discussed in more detail later in this document.

### AWS Global Regions

Data centers are built in clusters in various global regions. As of this writing, there are nine regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US) (Oregon), EU (Ireland), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), and South America (Sao Paulo).

## AWS Risk and Compliance Program

AWS provides information about its risk and compliance program to enable customers to incorporate AWS controls into their governance framework. This information can assist customers in documenting a complete control and governance framework with AWS included as an important part of that framework.

### Risk Management

AWS management has developed a strategic business plan which includes risk identification and the implementation of controls to mitigate or manage risks. AWS management re-evaluates the strategic business plan at least biannually. This process requires management to identify risks within its areas of responsibility and to implement appropriate measures designed to address those risks.

In addition, the AWS control environment is subject to various internal and external risk assessments. AWS's Compliance and Security teams have established an information security framework and policies based on the Control Objectives for Information and related Technology (COBIT) framework and have effectively integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, the PCI DSS v2.0, and the National Institute of Standards and Technology (NIST) Publication 800-53 Rev 3 (Recommended Security Controls for Federal Information Systems). AWS maintains the security policy, provides security

training to employees, and performs application security reviews. These reviews assess the confidentiality, integrity, and availability of data, as well as conformance to the information security policy.

AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership. These scans are done in a manner for the health and viability of the underlying AWS infrastructure and are not meant to replace the customer's own vulnerability scans required to meet their specific compliance requirements. Customers can request permission to conduct scans of their cloud infrastructure as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. Advance approval for these types of scans can be initiated by submitting a request via the AWS Vulnerability / Penetration Testing Request Form.

### Control Environment

AWS manages a comprehensive control environment that includes policies, processes and control activities that leverage various aspects of Amazon's overall control environment. This control environment is in place for the secure delivery of AWS's service offerings. The collective control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of AWS's control framework. AWS has integrated applicable cloud-specific controls identified by leading cloud computing industry bodies into the AWS control framework. AWS continues to monitor these industry groups for ideas on which leading practices can be implemented to better assist customers with managing their control environment.

The control environment at Amazon begins at the highest level of the Company. Executive and senior leadership play important roles in establishing the Company's tone and core values. Every employee is provided with the Company's Code of Business Conduct and Ethics and completes periodic training. Compliance audits are performed so that employees understand and follow the established policies.

The AWS organizational structure provides a framework for planning, executing and controlling business operations. The organizational structure assigns roles and responsibilities to provide for adequate staffing, efficiency of operations, and the segregation of duties. Management has also established authority and appropriate lines of reporting for key personnel. Included as part of the Company's hiring verification processes are education, previous employment, and, in some cases, background checks as permitted by law and regulation for employees commensurate with the employee's position and level of access to AWS facilities. The Company follows a structured on-boarding process to familiarize new employees with Amazon tools, processes, systems, policies and procedures.

### Information Security

AWS has implemented a formal information security program designed to protect the confidentiality, integrity, and availability of customers' systems and data. AWS publishes a security whitepaper that is available on the public website that addresses how AWS can help customers secure their data.

## AWS Reports, Certifications and Third-Party Attestations

AWS engages with external certifying bodies and independent auditors to provide customers with considerable information regarding the policies, processes, and controls established and operated by AWS.

## FedRAMP SM

AWS is a Federal Risk and Authorization Management Program (FedRAMP[sm]) Compliant Cloud Service Provider. AWS has completed the testing performed by a FedRAMP[sm] -accredited Third Party Assessment Organization (3PAO) and has been granted two Agency Authority to Operate (ATOs) by the US Department of Health and Human Services (HHS) after demonstrating compliance with FedRAMP[sm] requirements at the Moderate impact level. All U.S. government agencies can leverage the AWS Agency ATO packages stored in the FedRAMP[sm] repository to evaluate AWS for their applications and workloads, provide authorizations to use AWS, and transition workloads into the AWS environment. The two FedRAMP[sm] Agency ATOs encompass all U.S. regions (the AWS GovCloud (US) region and the AWS US East/West regions), and the following services are in the accreditation boundary for those regions: Amazon Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), Amazon Virtual Private Cloud (VPC), and Amazon Elastic Block Store (EBS). For more information on AWS FedRAMP[sm] compliance please see the AWS FedRAMP[sm] FAQs.

## FIPS 140-2

The Federal Information Processing Standard (FIPS) Publication 140-2 is a US government security standard that specifies the security requirements for cryptographic modules protecting sensitive information. To support customers with FIPS 140-2 requirements, the Amazon Virtual Private Cloud VPN endpoints and SSL-terminating load balancers in AWS GovCloud (US) operate using FIPS 140-2 validated hardware. AWS works with AWS GovCloud (US) customers to provide the information they need to help manage compliance with this requirement when using the AWS GovCloud (US) environment.

## FISMA and DIACAP

AWS enables US government agencies to achieve and sustain compliance with the Federal Information Security Management Act (FISMA). The AWS infrastructure has been evaluated by independent assessors for a variety of government systems as part of their system owners' approval process. Numerous Federal Civilian and Department of Defense (DoD) organizations have successfully achieved security authorizations for systems hosted on AWS in accordance with the Risk Management Framework (RMF) process defined in NIST 800-37 and DoD Information Assurance Certification and Accreditation Process (DIACAP). AWS's secure infrastructure has helped federal agencies expand cloud computing use cases and deploy sensitive government data and applications in the cloud while complying with the rigorous security requirements of federal standards.

## HIPAA

AWS enables covered entities and their business associates subject to the U.S. Health Insurance Portability and Accountability Act (HIPAA) to leverage the secure AWS environment to process, maintain, and store protected health information and AWS will be signing business associate agreements with such customers. AWS also offers a HIPAA-focused whitepaper for customers interested in learning more about how they can leverage AWS for the processing and storage of health information. The Creating HIPAA-Compliant Medical Data Applications with AWS whitepaper outlines how companies can use AWS to process systems that facilitate HIPAA and Health Information Technology for Economic and Clinical Health (HITECH) compliance.

## ISO 9001

AWS has achieved ISO 9001 certification, AWS's ISO 9001 certification directly supports customers who develop, migrate and operate their quality-controlled IT systems in the AWS cloud. Customers can leverage AWS's compliance reports as evidence for their own ISO 9001 programs and industry-specific quality programs, such as GxP in life sciences, ISO 13485

in medical devices, AS9100 in aerospace, and ISO/TS 16949 in automotive. AWS customers who don't have quality system requirements will still benefit from the additional assurance and transparency that an ISO 9001 certification provides The ISO 9001 certification covers the quality management system over a specified scope of AWS services and Regions of operations (below) and services including: AWS Direct Connect, Amazon DynamoDB, Amazon EC2 VM Import/Export, Amazon Elastic Block Store (EBS), Amazon Elastic Cloud Compute (EC2), Amazon Elastic MapReduce (EMR), Amazon ElastiCache, Amazon Glacier, AWS Identity and Access Management (IAM), Amazon Redshift, Amazon Relational Database Service (RDS), AWS Route 53, Amazon SimpleDB, Amazon Simple Storage Service (S3), AWS Storage Gateway, and Amazon Virtual Private Cloud (VPC). AWS's ISO 9001 accreditation covers AWS Regions including US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US), South America (Sãu Paulo), EU (Ireland), and Asia Pacific (Singapore), Asia Pacific (Sydney), and Asia Pacific (Tokyo).

ISO 9001:2008 is a global standard for managing the quality of products and services. The 9001 standard outlines a quality management system based on eight principles defined by the International Organization for Standardization (ISO) Technical Committee for Quality Management and Quality Assurance. They include:

- Customer focus
- Leadership
- Involvement of people
- Process approach
- System approach to management
- Continual Improvement
- Factual approach to decision-making
- Mutually beneficial supplier relationships

## ISO 27001

AWS has achieved ISO 27001 certification of our Information Security Management System (ISMS) covering AWS infrastructure, data centers, and services including: Amazon Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), Amazon Virtual Private Cloud (VPC), Amazon Elastic Block Store (EBS), Amazon Relational Database Service (RDS), Amazon DynamoDB, Amazon SimpleDB, Amazon Direct Connect, Amazon VM Import/Export, Amazon Glacier, and Amazon Storage Gateway. ISO 27001/27002 is a widely-adopted global security standard that sets out requirements and best practices for a systematic approach to managing company and customer information that’s based on periodic risk assessments appropriate to ever-changing threat scenarios. In order to achieve the certification, a company must show it has a systematic and ongoing approach to managing information security risks that affect the confidentiality, integrity, and availability of company and customer information. This certification reinforces Amazon’s commitment to providing significant information regarding our security controls and practices. AWS’s ISO 27001 certification includes all AWS data centers in all regions worldwide and AWS has established a formal program to maintain the certification. AWS provides additional information and frequently asked questions about its ISO 27001 certification on their web site.

## ITAR

The AWS GovCloud (US) region supports US International Traffic in Arms Regulations (ITAR) compliance. As a part of managing a comprehensive ITAR compliance program, companies subject to ITAR export regulations must control unintended exports by restricting access to protected data to US Persons and restricting physical location of that data to the US. AWS GovCloud (US) provides an environment physically located in the US and where access by AWS Personnel is limited to US Persons, thereby allowing qualified companies to transmit, process, and store protected articles and data

subject to ITAR restrictions. The AWS GovCloud (US) environment has been audited by an independent third-party to validate the proper controls are in place to support customer export compliance programs for this requirement.

## PCI DSS Level 1

AWS is Level 1 compliant under the Payment Card Industry (PCI) Data Security Standard (DSS). Customers can run applications on our PCI-compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud. In February 2013, the PCI Security Standards Council released PCI DSS Cloud Computing Guidelines. These guidelines provide customers who are managing a cardholder data environment with considerations for maintaining PCI DSS controls in the cloud. AWS has incorporated the PCI DSS Cloud Computing Guidelines into the AWS PCI Compliance Package for customers. The AWS PCI Compliance Package includes the AWS PCI Attestation of Compliance (AoC), which shows that AWS has been successfully validated against standards applicable to a Level 1 service provider under PCI DSS Version 2.0, and the AWS PCI Responsibility Summary, which explains how compliance responsibilities are shared between AWS and our customers in the cloud. The AWS PCI DSS Level 1 certification includes all The SOC 1 report scope covers: Amazon Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), Amazon Virtual Private Cloud (VPC), Amazon Elastic Block Store (EBS), Amazon Relational Database Service (RDS), Amazon DynamoDB, Amazon SimpleDB, Amazon Direct Connect, Amazon Glacier, Amazon Elastic MapReduce (EMR), and the infrastructure upon which they run for all regions worldwide. For more information on AWS PCI DSS compliance please visit PCI DSS Level 1 FAQs.

## SOC 1/SSAE 16/ISAE 3402

Amazon Web Services publishes a Service Organization Controls 1 (SOC 1), Type II report. The audit for this report is conducted in accordance with the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) and the International Standards for Assurance Engagements No. 3402 (ISAE 3402) professional standards. This dual-standard report is intended to meet a broad range of financial auditing requirements for U.S. and international auditing bodies. The SOC 1 report audit attests that AWS's control objectives are appropriately designed and that the individual controls defined to safeguard customer data are operating effectively. This report is the replacement of the Statement on Auditing Standards No. 70 (SAS 70) Type II Audit report.

The AWS SOC 1 control objectives are provided here. The report itself identifies the control activities that support each of these objectives and the independent auditor's results of their testing procedures of each control.

| Objective Area | Objective Description |
|---|---|
| **Security Organization** | Controls provide reasonable assurance that information security policies have been implemented and communicated throughout the organization. |
| **Amazon User Access** | Controls provide reasonable assurance that procedures have been established so that Amazon user accounts are added, modified and deleted in a timely manner and are reviewed on a periodic basis. |
| **Logical Security** | Controls provide reasonable assurance that unauthorized internal and external access to data is appropriately restricted and access to customer data is appropriately segregated from other customers. |
| **Secure Data Handling** | Controls provide reasonable assurance that data handling between the customer's point of initiation to an AWS storage location is secured and mapped accurately. |
| **Physical Security and Environmental Safeguards** | Controls provide reasonable assurance that physical access to Amazon's operations building and the data centers is restricted to authorized personnel and that procedures exist to minimize the effect of a malfunction or physical disaster to the computer and data center facilities. |

| | |
|---|---|
| **Change Management** | Controls provide reasonable assurance that changes (including emergency / non-routine and configuration) to existing IT resources are logged, authorized, tested, approved and documented. |
| **Data Integrity, Availability and Redundancy** | Controls provide reasonable assurance that data integrity is maintained through all phases including transmission, storage and processing. |
| **Incident Handling** | Controls provide reasonable assurance that system incidents are recorded, analyzed, and resolved. |

The SOC 1 reports are designed to focus on controls at a service organization that are likely to be relevant to an audit of a user entity's financial statements. As AWS's customer base is broad, and the use of AWS services is equally as broad, the applicability of controls to customer financial statements varies by customer. Therefore, the AWS SOC 1 report is designed to cover specific key controls likely to be required during a financial audit, as well as covering a broad range of IT general controls to accommodate a wide range of usage and audit scenarios. This allows customers to leverage the AWS infrastructure to store and process critical data, including that which is integral to the financial reporting process. AWS periodically reassesses the selection of these controls to consider customer feedback and usage of this important audit report.

AWS's commitment to the SOC 1 report is ongoing, and AWS will continue the process of periodic audits. The SOC 1 report scope covers: Amazon Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), Amazon Virtual Private Cloud (VPC), Amazon Elastic Block Store (EBS), Amazon Relational Database Service (RDS), Amazon DynamoDB, Amazon SimpleDB, Amazon Direct Connect, Amazon VM Import/Export, Amazon ElastiCache, Amazon Glacier, Amazon Storage Gateway, Amazon Elastic MapReduce (EMR), Amazon Redshift, AWS Identity and Access Management (IAM), and the infrastructure upon which they run for all regions worldwide.

## SOC 2

In addition to the SOC 1 report, AWS publishes a Service Organization Controls 2 (SOC 2), Type II report. Similar to the SOC 1 in the evaluation of controls, the SOC 2 report is an attestation report that expands the evaluation of controls to the criteria set forth by the American Institute of Certified Public Accountants (AICPA) Trust Services Principles. These principles define leading practice controls relevant to security, availability, processing integrity, confidentiality, and privacy applicable to service organizations such as AWS. The AWS SOC 2 is an evaluation of the design and operating effectiveness of controls that meet the criteria for the security principle set forth in the AICPA's Trust Services Principles criteria. This report provides additional transparency into AWS security based on a pre-defined industry standard of leading practices and further demonstrates AWS's commitment to protecting customer data. The SOC 2 report scope covers the same services covered in the SOC 1 report. See the SOC 1 description above for the in-scope services.

## SOC 3

AWS publishes a Service Organization Controls 3 (SOC 3) report. The SOC 3 report is a publically-available summary of the AWS SOC 2 report and provides the AICPA SysTrust Security Seal. The report includes the external auditor's opinion of the operation of controls (based on the AICPA's Security Trust Principles included in the SOC 2 report), the assertion from AWS management regarding the effectiveness of controls, and an overview of AWS Infrastructure and Services. The AWS SOC 3 report includes all AWS data centers worldwide that support in-scope services. This is a great resource for customers to validate that AWS has obtained external auditor assurance without going through the process to request a SOC 2 report. The SOC 3 report scope covers the same services covered in the SOC 1 report. See the SOC 1 description above for the in-scope services. View the AWS SOC 3 report here.

## Other Compliance Best Practices

The flexibility and customer control that the AWS platform provides permits the deployment of solutions that meet industry-specific compliance requirements.

- ***CSA***: AWS has completed the Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire. This questionnaire published by the CSA provides a way to reference and document what security controls exist in AWS's Infrastructure-as-a-Service offerings. The questionnaire (CAIQ) provides a set of over 140 questions a cloud consumer and cloud auditor may wish to ask of a cloud provider. See Appendix A of this document for the CSA Consensus Assessments Initiative Questionnaire completed by AWS.
- ***MPAA***: The Motion Picture Association of America (MPAA) has established a set of best practices for securely storing, processing and delivering protected media and content (http://www.fightfilmtheft.org/facility-security-program.html). Media companies use these best practices as a way to assess risk and security of their content and infrastructure. AWS has demonstrated alignment with the MPAA best practices and the AWS infrastructure is compliant with all applicable MPAA infrastructure controls. While the MPAA does not offer a "certification," media industry customers can use the AWS MPAA documentation to augment their risk assessment and evaluation of MPAA-type content on AWS. See Appendix B of this document for the AWS alignment with Motion Picture of America Association (MPAA) Content Security Model.

# Key Compliance Questions and AWS

This section addresses generic cloud computing compliance questions specifically for AWS. These common compliance questions listed may be of interest when evaluating and operating in a cloud computing environment and may assist in AWS customers' control management efforts.

| Ref | Cloud Computing Question | AWS Information |
|---|---|---|
| 1 | Control ownership. Who owns which controls for cloud-deployed infrastructure? | For the portion deployed into AWS, AWS controls the physical components of that technology. The customer owns and controls everything else, including control over connection points and transmissions. To help customers better understand what controls we have in place and how effectively they are operating, we publish a SOC 1 Type II report with controls defined around EC2, S3 and VPC, as well as detailed physical security and environmental controls. These controls are defined at a high level of specificity that should meet most customer needs. AWS customers that have signed a non-disclosure agreement with AWS may request a copy of the SOC 1 Type II report. |
| 2 | Auditing IT. How can auditing of the cloud provider be accomplished? | Auditing for most layers and controls above the physical controls remains the responsibility of the customer. The definition of AWS-defined logical and physical controls is documented in the SOC 1 Type II report (SSAE 16), and the report is available for review by audit and compliance teams. AWS ISO 27001 and other certifications are also available for auditors to review. |
| 3 | Sarbanes-Oxley compliance. How is SOX compliance achieved if in-scope systems are deployed in the cloud provider environment? | If a customer processes financial information in the AWS cloud, the customer's auditors may determine that some AWS systems come into scope for Sarbanes-Oxley (SOX) requirements. The customer's auditors must make their own determination regarding SOX applicability. Because most of the logical access controls are managed by customer, the customer is best positioned to determine if its control activities meet relevant standards. If the SOX auditors request specifics regarding AWS's physical controls, they can reference the AWS SOC 1 Type II report which details the controls that AWS provides. |
| 4 | HIPAA compliance. Is it possible to meet HIPAA compliance requirements while deployed in the cloud provider environment? | HIPAA requirements apply to and are controlled by the AWS customer. The AWS platform allows for the deployment of solutions that meet industry-specific certification requirements such as HIPAA. Customers can use AWS services to maintain a security level that is equivalent or greater than those required to protect electronic health records. Customers have built healthcare applications compliant with HIPAA's Security and Privacy Rules on AWS. AWS provides additional information about HIPAA compliance on its web site, including a whitepaper on this topic. |
| 5 | GLBA compliance. Is it possible to meet GLBA certification requirements while deployed in the cloud provider environment? | Most GLBA requirements are controlled by the AWS customer. AWS provides means for customers to protect data, manage permissions, and build GLBA-compliant applications on AWS infrastructure. If the customer requires specific assurance that physical security controls are operating effectively, they can reference the AWS SOC 1 Type II report as relevant. |

| Ref | Cloud Computing Question | AWS Information |
|---|---|---|
| 6 | Federal regulation compliance. Is it possible for a US Government agency to be compliant with security and privacy regulations while deployed in the cloud provider environment? | US Federal agencies can be compliant under a number of compliance standards, including the Federal Information Security Management Act (FISMA) of 2002, Federal Risk and Authorization Management Program (FedRAMP[sm]), the Federal Information Processing Standard (FIPS) Publication 140-2, and the International Traffic in Arms Regulations (ITAR). Compliance with other laws and statues may also be accommodated depending on the requirements set forth in the applicable legislation. |
| 7 | Data location. Where does customer data reside? | AWS customers designate in which physical region their data and their servers will be located. Data replication for S3 data objects is done within the regional cluster in which the data is stored and is not replicated to other data center clusters in other regions. AWS customers designate in which physical region their data and their servers will be located. AWS will not move customers' content from the selected Regions without notifying the customer, unless required to comply with the law or requests of governmental entities. As of this writing, there are nine regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US) (Oregon), EU (Ireland), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), and South America (Sao Paulo). |
| 8 | E-Discovery. Does the cloud provider meet the customer's needs to meet electronic discovery procedures and requirements? | AWS provides infrastructure, and customers manage everything else, including the operating system, the network configuration, and the installed applications. Customers are responsible for responding appropriately to legal procedures involving the identification, collection, processing, analysis, and production of electronic documents they store or process using AWS. Upon request, AWS may work with customers who require AWS's assistance in legal proceedings. |
| 9 | Data center tours. Are data center tours by customers allowed by the cloud provider? | No. Due to the fact that our data centers host multiple customers, AWS does not allow data center tours by customers, as this exposes a wide range of customers to physical access of a third party. To meet this customer need, an independent and competent auditor validates the presence and operation of controls as part of our SOC 1 Type II report (SSAE 16). This broadly accepted third-party validation provides customers with the independent perspective of the effectiveness of controls in place. AWS customers that have signed a non-disclosure agreement with AWS may request a copy of the SOC 1 Type II report. Independent reviews of data center physical security is also a part of the ISO 27001 audit, the PCI assessment, ITAR audit, and the FedRAMP[sm] testing programs. |
| 10 | Third party access. Are third parties allowed access to the cloud provider data centers? | AWS strictly controls access to data centers, even for internal employees. Third parties are not provided access to AWS data centers except when explicitly approved by the appropriate AWS data center manager per the AWS access policy. See the SOC 1 Type II report for specific controls related to physical access, data center access authorization, and other related controls. |
| 11 | Privileged actions. Are privileged actions monitored and controlled? | Controls in place limit access to systems and data and provide that access to systems or data is restricted and monitored. In addition, customer data is and server instances are logically isolated from other customers by default. Privileged user access control is reviewed by an independent auditor during the AWS SOC 1, ISO 27001, PCI, ITAR, and FedRAMP[sm] audits. |

| Ref | Cloud Computing Question | AWS Information |
|---|---|---|
| 12 | Insider access. Does the cloud provider address the threat of inappropriate insider access to customer data and applications? | AWS provides specific SOC 1 controls to address the threat of inappropriate insider access, and the public certification and compliance initiatives covered in this document address insider access. All certifications and third-party attestations evaluate logical access preventative and detective controls. In addition, periodic risk assessments focus on how insider access is controlled and monitored. |
| 13 | Multi-tenancy. Is customer segregation implemented securely? | The AWS environment is a virtualized, multi-tenant environment. AWS has implemented security management processes, PCI controls, and other security controls designed to isolate each customer from other customers. AWS systems are designed to prevent customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software. This architecture has been validated by an independent PCI Qualified Security Assessor (QSA) and was found to be in compliance with all requirements of PCI DSS version 2.0 published in October 2010.<br>Note that AWS also has single-tenancy options. Dedicated Instances are Amazon EC2 instances launched within your Amazon Virtual Private Cloud (Amazon VPC) that run hardware dedicated to a single customer. Dedicated Instances let you take full advantage of the benefits of Amazon VPC and the AWS cloud while isolating your Amazon EC2 compute instances at the hardware level. |
| 14 | Hypervisor vulnerabilities. Has the cloud provider addressed known hypervisor vulnerabilities? | Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor. The hypervisor is regularly assessed for new and existing vulnerabilities and attack vectors by internal and external penetration teams, and is well suited for maintaining strong isolation between guest virtual machines. The AWS Xen hypervisor security is regularly evaluated by independent auditors during assessments and audits. See the AWS security whitepaper for more information on the Xen hypervisor and instance isolation. |
| 15 | Vulnerability management. Are systems patched appropriately? | AWS is responsible for patching systems supporting the delivery of service to customers, such as the hypervisor and networking services. This is done as required per AWS policy and in accordance with ISO 27001, NIST, and PCI requirements. Customers control their own guest operating systems, software and applications and are therefore responsible for patching their own systems. |
| 16 | Encryption. Do the provided services support encryption? | Yes. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB, and EC2. IPSec tunnels to VPC are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Customers may also use third-party encryption technologies. Refer to the AWS Security white paper for more information. |
| 17 | Data ownership. What are the cloud provider's rights over customer data? | AWS customers retain control and ownership of their data. AWS errs on the side of protecting customer privacy and is vigilant in determining which law enforcement requests we must comply with. AWS does not hesitate to challenge orders from law enforcement if we think the orders lack a solid basis. |
| 18 | Data isolation. Does the cloud provider adequately isolate customer data? | All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. Amazon S3 provides advanced data access controls. Please see the AWS security whitepaper for more information about specific data services' security. |

| Ref | Cloud Computing Question | AWS Information |
|---|---|---|
| 19 | Composite services. Does the cloud provider layer its service with other providers' cloud services? | AWS does not leverage any third-party cloud providers to deliver AWS services to customers. |
| 20 | Physical and environmental controls. Are these controls operated by the cloud provider specified? | Yes. These are specifically outlined in the SOC 1 Type II report. In addition, other certifications AWS supports such as ISO 27001 and FedRAMP[sm] require best practice physical and environmental controls. |
| 21 | Client-side protection. Does the cloud provider allow customers to secure and manage access from clients, such as PC and mobile devices? | Yes. AWS allows customers to manage client and mobile applications to their own requirements. |
| 22 | Server security. Does the cloud provider allow customers to secure their virtual servers? | Yes. AWS allows customers to implement their own security architecture. See the AWS security whitepaper for more details on server and network security. |
| 23 | Identity and Access Management. Does the service include IAM capabilities? | AWS has a suite of identity and access management offerings, allowing customers to manage user identities, assign security credentials, organize users in groups, and manage user permissions in a centralized way. Please see the AWS web site for more information. |
| 24 | Scheduled maintenance outages. Does the provider specify when systems will be brought down for maintenance? | AWS does not require systems to be brought offline to perform regular maintenance and system patching. AWS's own maintenance and system patching generally do not impact customers. Maintenance of instances themselves is controlled by the customer. |
| 25 | Capability to scale. Does the provider allow customers to scale beyond the original agreement? | The AWS cloud is distributed, highly secure and resilient, giving customers massive scale potential. Customers may scale up or down, paying for only what they use. |
| 26 | Service availability. Does the provider commit to a high level of availability? | AWS does commit to high levels of availability in its service level agreements (SLA). For example, Amazon EC2 commits to annual uptime percentage of at least 99.95% during the service year. Amazon S3 commits to monthly uptime percentage of at least 99.9%. Service credits are provided in the case these availability metrics are not met. |
| 27 | Distributed Denial Of Service (DDoS) attacks. How does the provider protect their service against DDoS attacks? | The AWS network provides significant protection against traditional network security issues and the customer can implement further protection. See the AWS Security Whitepaper for more information on this topic, including a discussion of DDoS attacks. |
| 28 | Data portability. Can the data stored with a service provider be exported by customer request? | AWS allows customers to move data as needed on and off AWS storage. AWS Import/Export service for S3 accelerates moving large amounts of data into and out of AWS using portable storage devices for transport. |

| Ref | Cloud Computing Question | AWS Information |
|---|---|---|
| 29 | Service provider business continuity. Does the service provider operate a business continuity program? | AWS does operate a business continuity program. Detailed information is provided in the AWS Security Whitepaper. |
| 30 | Customer business continuity. Does the service provider allow customers to implement a business continuity plan? | AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance back-ups, data redundancy replication, and multi-region/availability zone deployment architectures. |
| 31 | Data durability. Does the service specify data durability? | Amazon S3 provides a highly durable storage infrastructure. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 Region. Once stored, Amazon S3 maintains the durability of objects by quickly detecting and repairing any lost redundancy. Amazon S3 also regularly verifies the integrity of data stored using checksums. If corruption is detected, it is repaired using redundant data. Data stored in S3 is designed to provide 99.999999999% durability and 99.99% availability of objects over a given year. |
| 32 | Backups. Does the service provide backups to tapes? | AWS allows customers to perform their own backups to tapes using their own tape backup service provider. However, a tape backup is not a service provided by AWS. Amazon S3 service is designed to drive the likelihood of data loss to near zero percent and the durability equivalent of multi-site copies of data objects is achieved through data storage redundancy. For information on data durability and redundancy, please refer to the AWS web site. |
| 33 | Price increases. Will the service provider raise prices unexpectedly? | AWS has a history of frequently reducing prices as the cost to provide these services reduces over time. AWS has reduced prices consistently over the past several years. |
| 34 | Sustainability. Does the service provider company have long term sustainability potential? | AWS is a leading cloud provider and is a long-term business strategy of Amazon.com. AWS has very high long term sustainability potential. |

## AWS Contact

Customers can request the reports and certifications produced by our third-party auditors or can request more information about AWS Compliance by contacting AWS Sales and Business Development. The representative will route customers to the proper team depending on nature of the inquiry. For additional information on AWS Compliance, see the AWS Compliance site or send questions directly to awscompliance@amazon.com.

# Appendix A: CSA Consensus Assessments Initiative Questionnaire v1.1

The Cloud Security Alliance (CSA) is a "not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing." [Reference **https://cloudsecurityalliance.org/about/**] A wide range of industry security practitioners, corporations, and associations participate in this organization to achieve its mission.

The CSA Consensus Assessments Initiative Questionnaire provides a set of questions the CSA anticipates a cloud consumer and/or a cloud auditor would ask of a cloud provider. It provides a series of security, control, and process questions which can then be used for a wide range of uses, including cloud provider selection and security evaluation. AWS has completed this questionnaire with the answers below.

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| Compliance | Audit Planning | CO-01.1 | Do you produce audit assertions using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)? | AWS obtains certain industry certifications and independent third party attestations and provides certain certifications, reports and other relevant documentation directly to AWS customers under NDA. |
| Compliance | Independent Audits | CO-02.1 | Do you allow tenants to view your SAS70 Type II/SSAE 16 SOC2/ISAE3402 or similar third party audit reports? | AWS provides third party attestations, certifications, Service Organization Controls 1 (SOC 1) Type II report and other relevant compliance reports directly to our customers under NDA.<br><br>AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership.<br><br>In addition, the AWS control environment is subject to regular internal and external risk assessments. AWS engages with external certifying bodies and independent auditors to review and test the AWS overall control environment. |
| Compliance | | CO-02.2 | Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance? | |
| Compliance | | CO-02.3 | Do you conduct regular application penetration tests of your cloud infrastructure as prescribed by industry best practices and guidance? | |
| Compliance | | CO-02.4 | Do you conduct internal audits regularly as prescribed by industry best practices and guidance? | |
| Compliance | | CO-02.5 | Do you conduct external audits regularly as prescribed by industry best practices and guidance? | |
| Compliance | | CO-02.6 | Are the results of the network penetration tests available to tenants at their request? | |
| Compliance | | CO-02.7 | Are the results of internal and external audits available to tenants at their request? | |
| Compliance | Third Party Audits | CO-03.1 | Do you permit tenants to perform independent vulnerability assessments? | Customers can request permission to conduct scans of their cloud infrastructure as long as they |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| Compliance | | CO-03.2 | Do you have external third-party conduct vulnerability scans and periodic penetration tests on your applications and networks? | are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. Advance approval for these types of scans can be initiated by submitting a request via the AWS Vulnerability / Penetration Testing Request Form.<br><br>AWS Security regularly engages independent security firms to perform external vulnerability threat assessments. The AWS SOC 1 Type II report provides additional details on the specific control activities executed by AWS. |
| Compliance | Contact / Authority Maintenance | CO-04.1 | Do you maintain liaisons and points of contact with local authorities in accordance with contracts and appropriate regulations? | AWS maintains contacts with industry bodies, risk and compliance organizations, local authorities and regulatory bodies as required by the ISO 27001 standard. |
| Compliance | Information System Regulatory Mapping | CO-05.1 | Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data? | All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. Customers retain control and ownership of their data, thus it is their responsibility to choose to encrypt the data. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB and EC2. IPSec tunnels to VPC are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security. |
| | | CO-05.2 | Do you have capability to logically segment and recover data for a specific customer in the case of a failure or data loss? | |
| Compliance | Intellectual Property | CO-06.1 | Do you have policies and procedures in place describing what controls you have in place to protect tenant's intellectual property? | AWS Compliance and Security teams have established an information security framework and policies based on the Control Objectives for Information and related Technology (COBIT) framework. The AWS security framework integrates the ISO 27002 best practices and the PCI Data Security Standard.<br><br>Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security. |
| Compliance | Intellectual Property | CO-07.1 | If utilization of tenants services housed in the cloud is mined for cloud provider benefit, are the tenants IP rights preserved? | Resource utilization is monitored by AWS as necessary to effectively manage the availability of the service. AWS does not collect customer's intellectual property as part of resource utilization monitoring. |
| Compliance | Intellectual Property | CO-08.1 | If utilization of tenants services housed in the cloud is mined for cloud provider benefit, do you provide tenants the ability to opt-out? | Utilization of customer services housed in the cloud is not mined. |
| Data Governance | Ownership / Stewardship | DG-01.1 | Do you follow a structured data-labeling standard (ex. ISO 15489, Oasis XML Catalog Specification, CSA data type guidance)? | AWS customers retain control and ownership of their data and may implement a structured data-labeling standard to meet their requirements. |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| Data Governance | Classification | DG-02.1 | Do you provide a capability to identify virtual machines via policy tags/metadata (ex. Tags can be used to limit guest operating systems from booting/instantiating/transporting data in the wrong country, etc.)? | Virtual Machines are assigned to customers as a part of the EC2 service. Customers retain control over what resources are being used and where resources reside. Refer to the AWS Website for additional details - http://aws.amazon.com. |
| Data Governance | | DG-02.2 | Do you provide a capability to identify hardware via policy tags/metadata/hardware tags (ex. TXT/TPM, VN-Tag, etc.)? | AWS provides the ability to tag EC2 resources. A form of metadata, EC2 tags can be used to create user-friendly names, enhance search-ability, and improve coordination between multiple users. The AWS Management Console has also supports tagging. |
| Data Governance | | DG-02.3 | Do you have a capability to use system geographic location as an authentication factor? | AWS provides the capability of conditional user access based on IP address. Customers can add conditions to control how users can use AWS, such as time of day, their originating IP address, or whether they are using SSL. |
| Data Governance | | DG-02.4 | Can you provide the physical location/geography of storage of a tenant's data upon request? | AWS provides customers the flexibility to place instances and store data within multiple geographic Regions. AWS customers designate in which physical region their data and their servers will be located. AWS will not move customers' content from the selected Regions without notifying the customer, unless required to comply with the law or requests of governmental entities. As of this writing, there are nine regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US) (Oregon), EU (Ireland), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), and South America (Sao Paulo). |
| Data Governance | | DG-02.5 | Do you allow tenants to define acceptable geographical locations for data routing or resource instantiation? | |
| Data Governance | Handling / Labeling / Security Policy | DG-03.1 | Are Policies and procedures established for labeling, handling and security of data and objects which contain data? | AWS customers retain control and ownership of their data and may implement a labeling and handing policy and procedures to meet their requirements. |
| Data Governance | | DG-03.2 | Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data? | |
| Data Governance | Retention Policy | DG-04.1 | Do you have technical control capabilities to enforce tenant data retention policies? | AWS provide customers with the ability to delete their data. However, AWS customers retain control and ownership of their data so it is the customer's responsibility to manage data |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| Data Governance | | DG-04.2 | Do you have a documented procedure for responding to requests for tenant data from governments or third parties? | retention to their own requirements. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.<br><br>AWS errs on the side of protecting customer privacy and is vigilant in determining which law enforcement requests we must comply with. AWS does not hesitate to challenge orders from law enforcement if we think the orders lack a solid basis. |
| Data Governance | Secure Disposal | DG-05.1 | Do you support secure deletion (ex. degaussing / cryptographic wiping) of archived data as determined by the tenant? | When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. |
| Data Governance | | DG-05.2 | Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of tenant data once a customer has exited your environment or has vacated a resource? | |
| Data Governance | Nonproduction Data | DG-06.1 | Do you have procedures in place to ensure production data shall not be replicated or used in non-production environments? | AWS customers retain control and ownership of their own data. AWS provides customers the ability to maintain and develop production and non-production environments. It is the responsibility of the customer to ensure that their production data is not replicated to non-production environments. |
| Data Governance | Information Leakage | DG-07.1 | Do you have controls in place to prevent data leakage or intentional/accidental compromise between tenants in a multi-tenant environment? | The AWS environment is a virtualized, multi-tenant environment. AWS has implemented security management processes, PCI controls, and other security controls designed to isolate each customer from other customers. AWS systems are designed to prevent customers from accessing physical hosts or instances not |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| Data Governance | | DG-07.2 | Do you have a Data Loss Prevention (DLP) or extrusion prevention solution in place for all systems which interface with your cloud service offering? | assigned to them by filtering through the virtualization software. This architecture has been validated by an independent PCI Qualified Security Assessor (QSA) and was found to be in compliance with all requirements of PCI DSS version 2.0 published in June 2011.<br><br>Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security. |
| Data Governance | Risk Assessments | DG-08.1 | Do you provide security control health data in order to allow tenants to implement industry standard Continuous Monitoring (which allows continual tenant validation of your physical and logical control status?) | AWS does publish independent auditor reports and certifications to provide customers with considerable information regarding the policies, processes, and controls established and operated by AWS. The relevant certifications and reports can be provided to AWS customers.<br><br>Continuous Monitoring of logical controls can be executed by customers on their own systems. |
| Facility Security | Policy | FS-01.1 | Can you provide evidence that policies and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas? | AWS engages with external certifying bodies and independent auditors to review and validate our compliance with compliance frameworks. AWS SOC 1 Type II report provides additional details on the specific physical security control activities executed by AWS. Refer to ISO 27001 standards; Annex A, domain 9.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| Facility Security | User Access | FS-02.1 | Pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background verification? | AWS conducts criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees commensurate with the employee's position and level of access to AWS facilities. |
| Facility Security | Controlled Access Points | FS-03.1 | Are physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented? | Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. The AWS SOC 1 Type II report provides additional details on the specific control activities executed by AWS. Refer to ISO 27001 standards; Annex A, domain 9.1 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| Facility Security | Secure Area Authorization | FS-04.1 | Do you allow tenants to specify which of your geographic locations their data is allowed to traverse into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)? | AWS customers can designate which physical region their data and their servers will be located. AWS will not move customers' content from the selected Regions without notifying the customer unless required to comply with the law or requests of governmental entities. As of this writing, there are nine regions: US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US) (Oregon), EU (Ireland), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), and South America (Sao Paulo). Refer to the AWS website at http://aws.amazon.com for additional details. |
| Facility Security | Unauthorized Persons Entry | FS-05.1 | Are ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises monitored, controlled and isolated from data storage and process? | Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. Refer to AWS Overview of Security Processes Whitepaper for further information available at http://aws.amazon.com/security. In addition, the AWS SOC 1 Type II report provides additional details on the specific control activities executed by AWS. |
| Facility Security | Offsite Authorization | FS-06.1 | Do you provide tenants with documentation that describes scenarios where data may be moved from one physical location to another? (ex. Offsite backups, business continuity failovers, replication) | AWS customers can designate which physical region their data will be located. AWS will not move customers' content from the selected Regions without notifying the customer unless required to comply with the law or requests of governmental entities.<br><br>Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| Facility Security | Offsite equipment | FS-07.1 | Do you provide tenants with documentation describing your policies and procedures governing asset management and repurposing of equipment? | In alignment with ISO 27001 standards, when a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices.<br><br>Refer to ISO 27001 standards; Annex A, domain 9.2 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| Facility Security | Asset Management | FS-08.1 | Do you maintain a complete inventory of all of your critical assets which includes ownership of the asset? | In alignment with ISO 27001 standards, AWS Hardware assets are assigned an owner, tracked and monitored by the AWS personnel with AWS proprietary inventory management tools. AWS procurement and supply chain team maintain relationships with all AWS suppliers.<br><br>Refer to ISO 27001 standards; Annex A, domain 7.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| Facility Security | | FS-08.2 | Do you maintain a complete inventory of all of your critical supplier relationships? | |
| Human Resources Security | Background Screening | HR-01.1 | Pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background verification? | AWS conducts criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees commensurate with the employee's position and level of access to AWS facilities.<br><br>Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. |
| Human Resources Security | Employment Agreements | HR-02.1 | Do you specifically train your employees regarding their role vs. the tenant's role in providing information security controls? | Every employee is provided with the Company's Code of Business Conduct and Ethics and completes periodic Information Security training which requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. |
| | | HR-02.2 | Do you document employee acknowledgment of training they have completed? | |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| Human Resources Security | Employment Termination | HR-03.1 | Are Roles and responsibilities for following performing employment termination or change in employment procedures assigned, documented and communicated? | AWS Human Resources team defines internal management responsibilities to be followed for termination and role change of employees and vendors. The responsibility for provisioning /de-provisioning employee and contractor access is shared across Human Resources (HR), Corporate Operations and Service Owners. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. |
| Information Security | Management Program | IS-01.1 | Do you provide tenants with documentation describing your Information Security Management Program (ISMP)? | AWS provides our customers with our ISO 27001 certification documentation that communicates AWS ISMS program. |
| Information Security | Management Support / Involvement | IS-02.1 | Are policies in place to ensure executive and line management take formal action to support information security through clear documented direction, commitment, explicit assignment and verification of assignment execution? | In alignment with ISO 27001 standards, policies and procedures have been established through AWS Information Security framework. The control environment at Amazon begins at the highest level of the Company. Executive and senior leadership play important roles in establishing the Company's tone and core values. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security. |
| Information Security | Policy | IS-03.1 | Do your information security and privacy policies align with particular industry standards (ISO-27001, ISO-22307, CoBIT, etc.)? | Policies and procedures have been established by AWS Information Security based upon the COBIT framework, ISO 27001 standards and the PCI DSS requirements.<br><br>AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. In addition AWS publishes a SOC 1 Type II report. Refer to the SOC 1 report for further details. The AWS Risk and Compliance whitepaper for additional details - available at http://aws.amazon.com/security. |
| | | IS-03.2 | Do you have agreements which ensure your providers adhere to your information security and privacy policies? | |
| | | IS-03.3 | Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards? | |
| Information Security | Baseline Requirements | IS-04.1 | Do you have documented information security baselines for every component of your infrastructure (ex. Hypervisors, operating systems, routers, DNS servers, etc.)? | In alignment with ISO 27001 standards, AWS maintains system baselines for critical components. Refer to ISO 27001 standards, Annex A, domain 12.1 and 15.2 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.<br><br>Customers can provide their own virtual machine image. VM Import enables customers to easily import virtual machine images from your existing environment to Amazon EC2 instances. |
| Information Security | | IS-04.2 | Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines? | |
| Information Security | | IS-04.3 | Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards? | |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| Information Security | Policy Reviews | IS-05.1 | Do you notify your tenants when you make material changes to your information security and/or privacy policies? | AWS Overview of Security Processes whitepaper and Risk and Compliance whitepapers, available at http://aws.amazon.com/security are updated on a regular basis to reflect updates to the AWS policies. |
| Information Security | Policy Enforcement | IS-06.1 | Is a formal disciplinary or sanction policy established for employees who have violated security policies and procedures? | AWS provides security policy and provides security training to employees to educate them as to their role and responsibilities concerning information security. Employees who violate Amazon standards or protocols are investigated and appropriate disciplinary action (e.g. warning, performance plan, suspension, and/or termination) is followed. Refer to the AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.<br><br>Refer to ISO 27001 Annex A, domain 8.2 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| Information Security | | IS-06.2 | Are employees made aware of what action might be taken in the event of a violation and stated as such in the policies and procedures? | |
| Information Security | User Access Policy | IS-07.1 | Do you have controls in place ensuring timely removal of systems access which is no longer required for business purposes? | Access is automatically revoked when an employee's record is terminated in Amazon's Human Resources system. When changes in an employee's job function occur, continued access must be explicitly approved to the resource or it will be automatically revoked. The AWS SOC 1 Type II report provides further details on User access revocation. In addition the AWS Security White paper, section "Employee Lifecycle" provides additional information.<br><br>Refer to ISO 27001 Annex A, domain 11 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| Information Security | | IS-07.2 | Do you provide metrics which track the speed with which you are able to remove systems access which is no longer required for business purposes? | |
| Information Security | User Access Restriction / Authorization | IS-08.1 | Do you document how you grant and approve access to tenant data? | AWS customers retain control and ownership of their data. Customers are responsible for the development, content, operation, maintenance, and use of their content. |
| Information Security | | IS-08.2 | Do you have a method of aligning provider and tenant data classification methodologies for access control purposes? | |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| Information Security | User Access Revocation | IS-09.1 | Is timely deprovisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or third parties? | Access is automatically revoked when an employee's record is terminated in Amazon's Human Resources system. When changes in an employee's job function occur, continued access must be explicitly approved to the resource or it will be automatically revoked. AWS SOC 1 Type II report provides further details on User access revocation. In addition the AWS Security White paper, section "Employee Lifecycle" provides additional information.<br><br>Refer to ISO 27001 Annex A, domain 11 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| Information Security | | IS-09.2 | Is any change in status intended to include termination of employment, contract or agreement, change of employment or transfer within the organization? | |
| Information Security | User Access Reviews | IS-10.1 | Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your tenants)? | In alignment with ISO 27001 standard, all access grants are reviewed every 90 days; explicit re-approval is required or access to the resource is automatically revoked. Controls specific to User Access reviews are outlined in the SOC 1 Type II report. Exceptions in the User entitlement controls are documented in the SOC 1 Type II report.<br><br>Refer to ISO 27001 standards, Annex A, domain 11.2 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| Information Security | | IS-10.2 | If users are found to have inappropriate entitlements, are all remediation and certification actions recorded? | |
| Information Security | | IS-10.3 | Will you share user entitlement remediation and certification reports with your tenants, if inappropriate access may have been allowed to tenant data? | |
| Information Security | Training / Awareness | IS-11.1 | Do you provide or make available a formal security awareness training program for cloud-related access and data management issues (i.e., multi-tenancy, nationality, cloud delivery model segregation of duties implications, and conflicts of interest) for all persons with access to tenant data? | In alignment with ISO 27001 standard, all AWS employees complete periodic Information Security training which requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. |
| Information Security | | IS-11.2 | Are administrators and data stewards properly educated on their legal responsibilities with regard to security and data integrity? | |
| Information Security | Industry Knowledge / Benchmarking | IS-12.1 | Do you participate in industry groups and professional associations related to information security? | AWS Compliance and Security teams maintain contacts with industry groups and professional services related to security. AWS has established an information security framework and policies |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| | | IS-12.2 | Do you benchmark your security controls against industry standards? | based upon the COBIT framework and have integrated the ISO 27001 certifiable framework based on ISO 27002 controls and the PCI DSS. Refer to the AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security. |
| Information Security | Roles / Responsibilities | IS-13.1 | Do you provide tenants with a role definition document clarifying your administrative responsibilities vs. those of the tenant? | The AWS Overview of Security Processes Whitepaper and the AWS Risk and Compliance Whitepaper provide details on the roles and responsibilities of AWS and those of our Customers. The whitepapers area available at: http://aws.amazon.com/security. |
| Information Security | Management Oversight | IS-14.1 | Are Managers responsible for maintaining awareness of and complying with security policies, procedures and standards that are relevant to their area of responsibility? | The Control environment at Amazon begins at the highest level of the Company. Executive and senior leadership play important roles in establishing the Company's tone and core values. Every employee is provided with the Company's Code of Business Conduct and Ethics and completes periodic training. Compliance audits are performed so that employees understand and follow the established policies. Refer to AWS Risk & Compliance whitepaper for additional details - available at http://aws.amazon.com/security. |
| Information Security | Segregation of Duties | IS-15.1 | Do you provide tenants with documentation on how you maintain segregation of duties within your cloud service offering? | Customers retain the ability to manage segregations of duties of their AWS resources.<br><br>Internally, AWS aligns with ISO 27001 standards for managing segregation of duties. Refer to ISO 27001 standard, Annex A, domain 10.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| Information Security | User Responsibility | IS-16.1 | Are users made aware of their responsibilities for maintaining awareness and compliance with published security policies, procedures, standards and applicable regulatory requirements? | AWS has implemented various methods of internal communication at a global level to help employees understand their individual roles and responsibilities and to communicate significant events in a timely manner. These methods include orientation and training programs for newly hired employee as well as electronic mail messages and the posting of information via the Amazon intranet. Refer to ISO 27001 standard, Annex A, domain 8.2 and 11.3. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. In addition the AWS Overview of Security Processes Whitepaper provides further details - available at http://aws.amazon.com/security. |
| Information Security | | IS-16.2 | Are users made aware of their responsibilities for maintaining a safe and secure working environment? | |
| Information Security | | IS-16.3 | Are users made aware of their responsibilities for leaving unattended equipment in a secure manner? | |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| Information Security | Workspace | IS-17.1 | Do your data management policies and procedures address tenant and service level conflicts of interests? | AWS data management policies are in alignment with ISO 27001 standard. Refer to ISO 27001 standard, Annex A, domain 8.2 and 11.3. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. AWS SOC 1 Type II report provides additional details on the specific control activities executed by AWS to prevent unauthorized access to AWS resources. |
| Information Security | | IS-17.2 | Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to tenant data? | |
| Information Security | | IS-17.3 | Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine? | |
| Information Security | Encryption | IS-18.1 | Do you have a capability to allow creation of unique encryption keys per tenant? | AWS Customers manage their own encryption unless they are utilizing AWS server side encryption service. In this case, AWS does create a unique encryption key per tenant. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. |
| Information Security | | IS-18.2 | Do you support tenant generated encryption keys or permit tenants to encrypt data to an identity without access to a public key certificate. (e.g. Identity based encryption)? | |
| Information Security | Encryption Key Management | IS-19.1 | Do you encrypt tenant data at rest (on disk/storage) within your environment? | AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB and EC2. IPSec tunnels to VPC are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Customers may also use third-party encryption technologies. AWS key management procedures are in alignment with ISO 27001 standard. Refer to ISO 27001 standard, Annex A, domain 15.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. |
| Information Security | | IS-19.2 | Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances? | |
| Information Security | | IS-19.3 | Do you have a capability to manage encryption keys on behalf of tenants? | |
| Information Security | | IS-19.4 | Do you maintain key management procedures? | |
| Information Security | Vulnerability / Patch Management | IS-20.1 | Do you conduct network-layer vulnerability scans regularly as prescribed by industry best practices? | Customers retain control of their own guest operating systems, software and applications and are responsible for performing vulnerability scans and patching of their own systems. Customers can request permission to conduct scans of their cloud infrastructure as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. AWS Security regularly scans all Internet-facing service endpoint IP addresses for vulnerabilities. AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. AWS's own maintenance and system patching generally do not impact customers. Refer to AWS Overview of Security Processes Whitepaper for |
| Information Security | | IS-20.2 | Do you conduct application-layer vulnerability scans regularly as prescribed by industry best practices? | |
| Information Security | | IS-20.3 | Do you conduct local operating system-layer vulnerability scans regularly as prescribed by industry best practices? | |
| Information Security | | IS-20.4 | Will you make the results of vulnerability scans available to tenants at their request? | |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| Information Security | | IS-20.5 | Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems? | further information - available at http://aws.amazon.com/security.<br><br>Refer to ISO 27001 standard, Annex A, domain 12.5 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| Information Security | | IS-20.6 | Will you provide your risk-based systems patching timeframes to your tenants upon request? | |
| Information Security | Antivirus / Malicious Software | IS-21.1 | Do you have anti-malware programs installed on all systems which support your cloud service offerings? | AWS's program, processes and procedures to managing antivirus / malicious software is in alignment with ISO 27001 standards. Refer to AWS SOC 1 Type II report provides further details.<br><br>In addition, refer to ISO 27001 standard, Annex A, domain 10.4 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| Information Security | | IS-21.2 | Do you ensure that security threat detection systems which use signatures, lists, or behavioral patterns are updated across all infrastructure components within industry accepted timeframes? | |
| Information Security | Incident Management | IS-22.1 | Do you have a documented security incident response plan? | AWS's incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. The AWS SOC 1 Type II report provides details on the specific control activities executed by AWS.<br><br>The AWS Overview of Security Processes whitepaper (available at http://aws.amazon.com/security) provides additional details. |
| Information Security | | IS-22.2 | Do you integrate customized tenant requirements into your security incident response plans? | |
| Information Security | | IS-22.3 | Do you publish a roles and responsibilities document specifying what you vs. your tenants are responsible for during security incidents? | |
| Information Security | Incident Reporting | IS-23.1 | Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting? | AWS's incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. AWS SOC 1 Type II report provides details on the specific control activities executed by AWS. All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities.<br><br>Refer to the AWS Overview of Security Processes whitepaper and the AWS Risk & Compliance whitepaper (available at http://aws.amazon.com/security) for additional details. |
| Information Security | | IS-23.2 | Does your logging and monitoring framework allow isolation of an incident to specific tenants? | |
| Information Security | Incident Response Legal Preparation | IS-24.1 | Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes & controls? | AWS's incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. AWS SOC 1 Type II report provides details on the specific control |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| Information Security | | IS-24.2 | Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques? | activities executed by AWS. All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities.<br><br>Refer to the AWS Overview of Security Processes whitepaper and the AWS Risk & Compliance whitepaper (available at http://aws.amazon.com/security) for additional details. |
| Information Security | | IS-24.3 | Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific tenant without freezing other tenant data? | |
| Information Security | | IS-24.4 | Do you enforce and attest to tenant data separation when producing data in response to legal subpoenas? | |
| Information Security | Incident Response Metrics | IS-25.1 | Do you monitor and quantify the types, volumes, and impacts on all information security incidents? | AWS Security Metrics are monitored and analyzed in accordance with ISO 27001 standard.<br><br>Refer to ISO 27001 Annex A, domain 13.2 for further details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| Information Security | | IS-25.2 | Will you share statistical information security incident data with your tenants upon request? | |
| Information Security | Acceptable Use | IS-26.1 | Do you provide documentation regarding how you may utilize or access tenant data and/or metadata? | AWS customers retain control and ownership of their data. |
| Information Security | | IS-26.2 | Do you collect or create metadata about tenant data usage through the use of inspection technologies (search engines, etc.)? | |
| Information Security | | IS-26.3 | Do you allow tenants to opt-out of having their data/metadata accessed via inspection technologies? | |
| Information Security | Asset Returns | IS-27.1 | Are systems in place to monitor for privacy breaches and notify tenants expeditiously if a privacy event may have impacted their data? | AWS customers retain the responsibility to monitor their own environment for privacy breaches.<br><br>AWS SOC 1 Type II report provides an overview of the controls in place to monitor AWS managed environment. |
| Information Security | | IS-27.2 | Is your Privacy Policy aligned with industry standards? | |
| Information Security | eCommerce Transactions | IS-28.1 | Do you provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to traverse public networks? (ex. the Internet) | All of the AWS APIs are available via SSL-protected endpoints which provide server authentication. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB and EC2. IPSec tunnels to VPC are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Customers may also use third-party encryption technologies.<br><br>Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. |
| Information Security | | IS-28.2 | Do you utilize open encryption methodologies any time your infrastructure components need to communicate to each other over public networks (ex. Internet-based replication of data from one environment to another)? | |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| Information Security | Audit Tools Access | IS-29.1 | Do you restrict, log, and monitor access to your information security management systems? (Ex. Hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.) | In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC 1 Type II report outlines the controls in place to manage access provisioning to AWS resources.<br><br>Refer to AWS Overview of Security Processes whitepaper for additional details - available at http://aws.amazon.com/security. |
| Information Security | Diagnostic / Configuration Ports Access | IS-30.1 | Do you utilize dedicated secure networks to provide management access to your cloud service infrastructure? | Administrators with a business need to access the management plane are required to use multifactor authentication to gain access to purpose-built administration hosts. These administrative hosts are systems that are specifically designed, built, configured, and hardened to protect the management plane of the cloud. All such access is logged and audited. When an employee no longer has a business need to access the management plane, the privileges and access to these hosts and relevant systems are revoked. |
| Information Security | Network / Infrastructure Services | IS-31.1 | Do you collect capacity and utilization data for all relevant components of your cloud service offering? | AWS manages capacity and utilization data in alignment with ISO 27001 standard.<br><br>AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| Information Security | | IS-31.2 | Do you provide tenants with capacity planning and utilization reports? | |
| Information Security | Portable / Mobile Devices | IS-32.1 | Are Policies and procedures established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the provider organization's facilities)? | In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC 1 Type II report outlines the controls in place to manage access provisioning to AWS resources.<br><br>Refer to AWS Overview of Security Processes for additional details - available at http://aws.amazon.com/security. |
| Information Security | Source Code Access Restriction | IS-33.1 | Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only? | In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC 1 Type II report outlines the controls in place to manage access provisioning to AWS resources.<br><br>Refer to AWS Overview of Security Processes for additional details - available at http://aws.amazon.com/security. |
| Information Security | | IS-33.2 | Are controls in place to prevent unauthorized access to tenant application, program or object source code, and assure it is restricted to authorized personnel only? | |
| Information Security | Utility Programs Access | IS-34.1 | Are utilities that can significantly manage virtualized partitions (ex. shutdown, clone, etc.) appropriately restricted and monitored? | In alignment with ISO 27001 standards, system utilities are appropriately restricted and monitored. AWS SOC 1 Type II report provides additional details on controls in place to restrict |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| Information Security | | IS-34.2 | Do you have a capability to detect attacks which target the virtual infrastructure directly (ex. shimming, Blue Pill, Hyper jumping, etc.)? | system access.<br><br>Refer to AWS Overview of Security Processes for additional details - available at http://aws.amazon.com/security. |
| Information Security | | IS-34.3 | Are attacks which target the virtual infrastructure prevented with technical controls? | |
| Legal | Nondisclosure Agreements | LG-01.1 | Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified, documented and reviewed at planned intervals? | Amazon Legal Counsel manages and periodically revises the Amazon NDA to reflect AWS business needs. |
| Legal | Third Party Agreements | LG-02.1 | Do you select and monitor outsourced providers in compliance with laws in the country where the data is processed and stored and transmitted? | AWS does not leverage any third-party cloud providers to deliver AWS services to customers.<br><br>Third party agreements are reviewed by Amazon Legal Counsel as appropriate. |
| Legal | | LG-02.2 | Do you select and monitor outsourced providers in compliance with laws in the country where the data originates? | |
| Legal | | LG-02.3 | Does legal counsel review all third party agreements? | |
| Operations Management | Policy | OP-01.1 | Are policies and procedures established and made available for all personnel to adequately support services operations roles? | Policies and Procedures have been established through AWS Information Security framework based upon the COBIT framework, ISO 27001 standard and the PCI DSS requirements.<br><br>Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security. |
| Operations Management | Documentation | OP-02.1 | Are Information system documentation (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure Configuring, installing, and operating the information system? | Information System Documentation is made available internal to AWS personnel through the use of Amazon's Intranet site. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. |
| Operations Management | Capacity / Resource Planning | OP-03.1 | Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios? | AWS does not disclose capacity management practices. AWS publishes service level agreements for services to communicate performance level commitments. |
| Operations Management | | OP-03.2 | Do you restrict use of the memory oversubscription capabilities present in the hypervisor? | |
| Operations Management | Equipment Maintenance | OP-04.1 | If using virtual infrastructure, does your cloud solution include hardware independent restore and recovery capabilities? | EBS Snapshot functionality allows customers to capture and restore virtual machine images at any time. Customers can export their AMIs and use them on premise or at another provider |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| Operations Management | | OP-04.2 | If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time? | (subject to software licensing restrictions). Refer to the AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. |
| Operations Management | | OP-04.3 | If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider? | |
| Operations Management | | OP-04.4 | If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location? | |
| Operations Management | | OP-04.5 | Does your cloud solution include software / provider independent restore and recovery capabilities? | |
| Risk Management | Program | RI-01.1 | Is your organization insured by a 3rd party for losses? | AWS provides customer remuneration for losses they may incur due to outages in alignment with AWS's Service Level Agreement. |
| Risk Management | | RI-01.2 | Do your organization's service level agreements provide tenant remuneration for losses they may incur due to outages or losses experienced within your infrastructure? | |
| Risk Management | Assessments | RI-02.1 | Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods? | In alignment with ISO 27001 AWS has developed a Risk Management program to mitigate and manage risk.<br><br>AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification.<br><br>Refer to AWS Risk and Compliance Whitepaper (available at aws.amazon.com/security) for additional details on AWS Risk Management Framework. |
| Risk Management | | RI-02.2 | Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)? | |
| Risk Management | Mitigation / Acceptance | RI-03.1 | Are risks mitigated to acceptable levels based on company-established criteria in accordance with reasonable resolution time frames? | In alignment with ISO 27001 standard, Annex A, domain 4.2, AWS has developed a Risk Management program to mitigate and manage risk.<br><br>AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification.<br><br>Refer to AWS Risk and Compliance Whitepaper (available at: http://aws.amazon.com/security) |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| | | RI-03.2 | Is remediation conducted at acceptable levels based on company-established criteria in accordance with reasonable time frames? | for additional details on AWS Risk Management Framework |
| Risk Management | Business / Policy Change Impacts | RI-04.1 | Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective? | Updates to AWS security policies, procedures, standards and controls occur on an annual basis in alignment with the ISO 27001 standard.<br><br>Refer to ISO 27001 Annex A, domain 5.1 for additional information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification. |
| Risk Management | Third Party Access | RI-05.1 | Do you provide multi-failure disaster recovery capability? | AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. In case of failure, automated processes move customer data traffic away from the affected area. AWS SOC 1 Type II report provides further details. ISO 27001 standard Annex A, domain 11. 2 provides additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification. |
| | | RI-05.2 | Do you monitor service continuity with upstream providers in the event of provider failure? | |
| | | RI-05.3 | Do you have more than one provider for each service you depend on? | |
| | | RI-05.4 | Do you provide access to operational redundancy and continuity summaries which include the services on which you depend? | |
| | | RI-05.5 | Do you provide the tenant the ability to declare a disaster? | |
| | | RI-05.6 | Do you provide a tenant triggered failover option? | |
| | | RI-05.7 | Do you share your business continuity and redundancy plans with your tenants? | |
| Release Management | New Development / Acquisition | RM-01.1 | Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities? | In alignment with ISO 27001 standards, AWS has in place procedures to manage new development of resources.<br><br>AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification. In addition AWS SOC 1 Type II report provides further information. |
| Release Management | Production Changes | RM-02.1 | Do you provide tenants with documentation which describes your production change management procedures and their roles/rights/responsibilities within it? | AWS SOC 1 Type II report provides an overview of the controls in place to manage change Management in the AWS environment.<br><br>In addition, refer to ISO 27001 standard, Annex A, domain 12.5 for further details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| Release Management | Quality Testing | RM-03.1 | Do you provide your tenants with documentation which describes your quality assurance process? | AWS incorporates standards of quality as part of the system development lifecycle (SDLC) processes which are in alignment with ISO 27001 standard.<br><br>Refer to ISO 27001 standard, Annex A, domain 10.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| Release Management | Outsourced Development | RM-04.1 | Do you have controls in place to ensure that standards of quality are being met for all software development? | AWS does not generally outsource development of software. AWS incorporates standards of quality as part of the system development lifecycle (SDLC) processes which are in alignment with ISO 27001 standard.<br><br>Refer to ISO 27001 standard, Annex A, domain 10.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| Release Management | | RM-04.2 | Do you have controls in place to detect source code security defects for any outsourced software development activities? | |
| Release Management | Unauthorized Software Installations | RM-05.1 | Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems? | AWS's program, processes and procedures for managing malicious software is in alignment with ISO 27001 standards. Refer to AWS SOC 1 Type II report provides further details.<br><br>In addition, refer to ISO 27001 standard, Annex A, domain 10.4 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| Resiliency | Management Program | RS-01.1 | Are Policy, process and procedures defining business continuity and disaster recovery in place to minimize the impact of a realized risk event and properly communicated to tenants? | AWS Business Continuity Policies and Plans have been developed and tested in alignment with ISO 27001 standards.<br><br>Refer to ISO 27001 standard, annex A domain 14.1 and AWS SOC 1 report for further details on AWS and business continuity. |
| Resiliency | Impact Analysis | RS-02.1 | Do you provide tenants with ongoing visibility and reporting into your operational Service Level Agreement (SLA) performance? | AWS Cloudwatch provides monitoring for AWS cloud resources and the applications customers run on AWS. Refer to aws.amazon.com/cloudwatch for additional details. AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to status.aws.amazon.com. |
| Resiliency | | RS-02.2 | Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants? | |
| Resiliency | | RS-02.3 | Do you provide customers with ongoing visibility and reporting into your SLA performance? | |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| Resiliency | Business Continuity Planning | RS-03.1 | Do you provide tenants with geographically resilient hosting options? | Data centers are built in clusters in various global regions. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones.<br><br>Refer to AWS Overview of Security Processes whitepaper for additional details - available at http://aws.amazon.com/security |
| Resiliency | | RS-03.2 | Do you provide tenants with infrastructure service failover capability to other providers? | |
| Resiliency | Business Continuity Testing | RS-04.1 | Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness? | AWS Business Continuity Plans have been developed and tested in alignment with ISO 27001 standards.<br><br>Refer to ISO 27001 standard, annex A domain 14.1 and AWS SOC 1 report for further details on AWS and business continuity. |
| Resiliency | Environmental Risks | RS-05.1 | Is physical protection against damage from natural causes and disasters as well as deliberate attacks anticipated, designed and countermeasures applied? | AWS data centers incorporate physical protection against environmental risks. AWS's physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices.<br><br>Refer to ISO 27001 standard, Annex A domain 9.1 and the AWS SOC 1 Type II report for additional information. |
| Resiliency | Equipment Location | RS-06.1 | Are any of your data centers located in places which have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)? | AWS data centers incorporate physical protection against environmental risks. AWS services provide customers the flexibility to store data within multiple geographical regions as well as across multiple Availability zones. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones.<br><br>Refer to ISO 27001 standard, Annex A domain 9.1 and the AWS SOC 1 Type II report for additional information. |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| Resiliency | Equipment Power Failures | RS-07.1 | Are Security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)? | AWS equipment is protected from outages in alignment with ISO 27001 standard. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.<br><br>AWS SOC 1 Type II report provides additional details on controls in place to minimize the effect of a malfunction or physical disaster to the computer and data center facilities.<br><br>In addition, refer to the AWS Overview of Security Processes Whitepaper - available at http://aws.amazon.com/security. |
| Resiliency | Power / Telecommunications | RS-08.1 | Do you provide tenants with documentation showing the transport route of their data between your systems? | AWS customers designate in which physical region their data and servers will be located. AWS will not move customers' content from the selected Regions without notifying the customer, unless required to comply with the law or requests of governmental entities. AWS SOC 1 Type II report provides additional details. Customers can also choose their network path to AWS facilities, including over dedicated, private networks where the customer controls the traffic routing. |
| Resiliency | | RS-08.2 | Can Tenants define how their data is transported and through which legal jurisdiction? | |
| Security Architecture | Customer Access Requirements | SA-01.1 | Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems? | AWS customers retain responsibility to ensure their usage of AWS is within compliance of applicable laws and regulations. AWS communicates its security and control environment to customers through industry certifications and third party attestations, white papers (available at http://aws.amazon.com/security) and providing certifications, reports and other relevant documentation directly to AWS customers.<br><br>Refer to ISO 27001 standard, Annex A, domain 6.2 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| Security Architecture | User ID Credentials | SA-02.1 | Do you support use of, or integration with, existing customer-based Single Sign On (SSO) solutions to your service? | The AWS Identity and Access Management (IAM) service provides identity federation to the AWS Management Console. Multi-factor authentication is an optional feature that a customer can utilize. Refer to the AWS website for additional details - http://aws.amazon.com/mfa. |
| Security Architecture | | SA-02.2 | Do you use open standards to delegate authentication capabilities to your tenants? | |
| Security Architecture | | SA-02.3 | Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users? | |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| Security Architecture | | SA-02.4 | Do you have a Policy Enforcement Point capability (ex. XACML) to enforce regional legal and policy constraints on user access? | |
| Security Architecture | | SA-02.5 | Do you have an identity management system in place which enables both role-based and context-based entitlement to data (enables classification of data for a tenant)? | |
| Security Architecture | | SA-02.6 | Do you provide tenants with strong (multifactor) authentication options (digital certs, tokens, biometric, etc..) for user access? | |
| Security Architecture | | SA-02.7 | Do you allow tenants to use third party identity assurance services? | |
| Security Architecture | Data Security / Integrity | SA-03.1 | Is your Data Security Architecture designed using an industry standard? (ex. CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP[sm] CAESARS) | AWS Data Security Architecture was designed to incorporate industry leading practices.<br><br>Refer to ISO 27001 standard, Annex A, domain 10.8 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| Security Architecture | Application Security | SA-04.1 | Do you utilize industry standards (Build Security in Maturity Model [BSIMM] Benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build-in security for your Systems/Software Development Lifecycle (SDLC)? | The AWS system development lifecycle incorporates industry best practices which include formal design reviews by the AWS Security Team, threat modeling and completion of a risk assessment. Refer to the AWS Overview of Security Processes for further details.<br><br>In addition, refer to ISO 27001 standard, Annex A, domain 12.5 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| Security Architecture | | SA-04.2 | Do you utilize an automated source-code analysis tool to detect code security defects prior to production? | |
| Security Architecture | | SA-04.3 | Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security? | |
| Security Architecture | Data Integrity | SA-05.1 | Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data? | AWS data integrity controls as described in AWS SOC 1 Type II report provides reasonable assurance that data integrity is maintained through all phases including transmission, storage and processing.<br><br>In addition, refer to ISO 27001 standard, Annex A, domain 12.2 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| Security Architecture | Production / Nonproduction Environments | SA-06.1 | For your SaaS or PaaS offering, do you provide tenants with separate environments for production and test processes? | AWS Customers retain the ability and the responsibility to create and maintain production and test environments. AWS website provides guidance on creating an environment utilizing the AWS services - http://aws.amazon.com/documentation/. |
| Security Architecture | | SA-06.2 | For your IaaS offering, do you provide tenants with guidance on how to create suitable production and test environments? | |
| Security Architecture | Remote User Multifactor Authentication | SA-07.1 | Is multi-factor authentication required for all remote user access? | Multi-factor authentication is an optional feature that a Customer can utilize. Refer to the AWS website for additional details - http://aws.amazon.com/mfa. |
| Security Architecture | Network Security | SA-08.1 | For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution? | The AWS website provides guidance on creating a layered security architecture in a number of white papers available via the AWS public website - http://aws.amazon.com/documentation/. |
| Security Architecture | Segmentation | SA-09.1 | Are system and network environments logically separated to ensure Business and customer security requirements? | AWS customers retain responsibility to manage their own network segmentation in adherence with their defined requirements.<br><br>Internally, AWS network segmentation is aligned with ISO 27001 standards. Refer to ISO 27001 standard, Annex A. domain 11.4 for further detail. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| Security Architecture | | SA-09.2 | Are system and network environments logically separated to ensure compliance with legislative, regulatory, and contractual requirements? | |
| Security Architecture | | SA-09.3 | Are system and network environments logically separated to ensure separation of production and non-production environments? | |
| Security Architecture | | SA-09.4 | Are system and network environments logically separated to ensure protection and isolation of sensitive data? | |
| Security Architecture | Wireless Security | SA-10.1 | Are policies and procedures established and mechanisms implemented to protect network environment parameter and configured to restrict unauthorized traffic? | Policies, procedures and mechanisms to protect AWS network environment are in place. AWS SOC 1 Type II report provides additional details.<br><br>In addition refer to ISO 27001 standard, Annex A, domain 10.6 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| Security Architecture | | SA-10.2 | Are policies and procedures established and mechanisms implemented to ensure proper security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings, etc.) | |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| Security Architecture | | SA-10.3 | Are policies and procedures established and mechanisms implemented to protect network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network? | |
| Security Architecture | Shared Networks | SA-11.1 | Is access to systems with shared network infrastructure restricted to authorized personnel in accordance with security policies, procedures and standards. Networks shared with external entities shall have a documented plan detailing the compensating controls used to separate network traffic between organizations? | Access is strictly restricted to critical resources including services, hosts, and network devices and must be explicitly approved in Amazon's proprietary permission management system. AWS SOC 1 Type II report provides additional details on the specific control activities executed by AWS.<br><br>In addition, refer to ISO 27001 standard, Annex A, domain 11. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| Security Architecture | Clock Synchronization | SA-12.1 | Do you utilize a synchronized time-service protocol (ex. NTP) to ensure all systems have a common time reference? | In alignment with ISO 27001 standards, AWS information systems utilize internal system clocks synchronized via NTP (Network Time Protocol).<br><br>AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| Security Architecture | Equipment Identification | SA-13.1 | Is automated equipment identification used as a method of connection authentication to validate connection authentication integrity based on known equipment location? | AWS manages equipment identification in alignment with ISO 27001 standard.<br><br>AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| Security Architecture | Audit Logging / Intrusion Detection | SA-14.1 | Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents? | AWS Incident response program (detection, investigation and response to incidents) have been developed in alignment with ISO 27001 standard. AWS SOC 1 Type II report provides details on the specific control activities executed by AWS.<br><br>The AWS Overview of Security Processes whitepaper (available at http://aws.amazon.com/security) provides additional details. |
| Security Architecture | | SA-14.2 | Is Physical and logical user access to audit logs restricted to authorized personnel? | |
| Security Architecture | | SA-14.3 | Can you provide evidence that due diligence mapping of regulations and standards to your controls/architecture/processes has been done? | |
| Security Architecture | Mobile Code | SA-15.1 | Is mobile code authorized before its installation and use and the code configuration checked to ensure that the authorized mobile code operates according to a clearly defined security policy? | AWS allows customers to manage client and mobile applications to their own requirements. |

| Domain | Control Group | CID | Consensus Assessment Questions | AWS Response |
|---|---|---|---|---|
| Security Architecture | | SA-15.2 | Is all unauthorized mobile code prevented from executing? | |

# Appendix B: AWS alignment with Motion Picture of America Association (MPAA) Content Security Model

The Motion Picture of America Association (MPAA) has established a set of best practices for securely storing, processing and delivering protected media and content. For additional information on MPAA content security best practices refer to: http://www.fightfilmtheft.org/best-practice.html
Media Companies can utilize these best practices as a way to assess risk and audit security of the content management.
The table below documents AWS alignment with Motion Picture of America Association (MPAA) Content Security Model Guidelines released January 1, 2013. For additional information a reference to AWS third party audited certifications and reports is provided.
* The ISO 27002 and NIST 800-53 mapping is captured as defined in the *"MPAA Content Security Best Practices Common Guidelines January 1, 2013"*

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| MS-1.0 | Executive Security Awareness/ Oversight | Ensure executive management/owner(s) oversight of the Information Security function by requiring periodic review of the information security program and risk assessment results | The Control environment at Amazon begins at the highest level of the Company. Executive and senior leadership play important roles in establishing the Company's tone and core values. AWS has established an information security framework and policies based on the Control Objectives for Information and related Technology (COBIT) framework and have effectively integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, the PCI DSS v2.0 and the National Institute of Standards and Technology (NIST) Publication 800-53 Rev 3 (Recommended Security Controls for Federal Information Systems). AWS employee's complete periodic role based training which includes AWS Security training. Compliance audits are performed so that employees understand and follow the established policies. | MS-1 | SOC1 (1.1) SOC2 (S.2.3) | 4.1 6.11 | 12.4 12.5 | PM-1 PM-2 |
| MS.S-1.0 | Executive Security Awareness / Oversight | Establish an information security management system that implements a control framework (e.g., IS0 27001) for information security which is approved by executive management/owner(s) | | | | | | |
| MS-1.1 | Executive Security Awareness/ Oversight | Train and engage executive management/owner(s) on the business' responsibilities to protect content | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| MS-2.0 | Risk Management | Develop a formal security risk assessment process focused on content workflows and sensitive assets in order to identify and prioritize risks of content theft and leakage that are relevant to the facility | AWS has implemented a formal, documented risk assessment policy that is updated and reviewed at least annually. This policy addresses purpose, scope, roles, responsibilities, and management commitment.<br><br>In alignment with this policy, an annual risk assessment which covers all AWS regions and businesses is conducted by the AWS Compliance team and reviewed by AWS Senior Management. This is in addition to the Certification, attestation and reports that are conducted by independent auditors. The purpose of the risk assessment is to identify threats and vulnerabilities of AWS, to assign the threats and vulnerabilities a risk rating, to formally document the assessment, and to create a risk treatment plan for addressing issues. Risk assessment results are reviewed by the AWS Senior Management on an annual basis and when a significant change warrants a new risk assessment prior to the annual risk assessment.<br><br>Customers retain ownership of their data (content) and are responsible for assessing and managing risk associated with the workflows of their data to meet their compliance needs.<br><br>The AWS Risk Management framework is reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP[sm] compliance. | MS-2 | SOC2 (S3.31, S4.2, S4.3) | 4.1<br>4.2<br>7.2 | 12.1<br>12.2 | CA-1<br>CA-2<br>CA-5<br>RA-1<br>RA-2<br>RA-3 |
| MS-2.1 | Risk Management | Identify high-security content based on client instruction | | | | | | |
| MS-2.2 | Risk Management | Conduct an internal risk assessment annually and upon key workflow changes—based on, at a minimum, the MPAA Best Practice Common Guidelines and the applicable Supplemental Guidelines—and document and act upon identified risks | | | | | | |
| MS-3.0 | Security Organization | Identify security key point(s) of contact and formally define roles and responsibilities for content and asset protection | AWS has an established information security organization managed by the AWS Security team and is led by the AWS Chief Information Security Officer (CISO). AWS maintains and provides security awareness training to all information system users supporting AWS. This annual security awareness training includes the following topics; The purpose for security and awareness training, The location of all AWS policies, AWS incident response procedures | MS-3 | SOC1 (1.1)<br>SOC2 (S.2.3) | 6.1.3 | 12.4<br>12.5 | PM-2 |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| MS.S-3.0 | Security Organization | Establish a security team that is responsible for proactively monitoring information systems and physical security to identify and respond to any suspicious activity | (including instructions on how to report internal and external security incidents).<br><br>Systems within AWS are extensively instrumented to monitor key operational and security metrics. Alarms are configured to automatically notify operations and management personnel when early warning thresholds are crossed on key metrics. When a threshold is crossed, the AWS incident response process is initiated. The Amazon Incident Response team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Staff operates 24x7x365 coverage to detect incidents and manage the impact to resolution.<br><br>AWS roles & Responsibilities are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP[sm] compliance | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| MS-4.0 | Policies and Procedures | Establish policies and procedures regarding asset and content security; policies should address the following topics, at a minimum:<br>• Human resources policies<br>• Acceptable use (e.g., social networking, Internet, phone, etc.)<br>• Asset classification<br>• Asset handling policies<br>• Digital recording devices (e.g., smart phones, digital cameras, camcorders)<br>• Exception policy (e.g., process to document policy deviations)<br>• Password controls (e.g., password minimum length, screensavers)<br>• Prohibition of client asset removal from the facility<br>• System change management<br>• Whistleblower policy<br>• Sanction policy (e.g., disciplinary policy) | AWS has established an information security framework and policies based on the Control Objectives for Information and related Technology (COBIT) framework and have effectively integrated the ISO 27001 certifiable framework based on ISO 27002 controls, American Institute of Certified Public Accountants (AICPA) Trust Services Principles, the PCI DSS v2.0 and the National Institute of Standards and Technology (NIST) Publication 800-53 Rev 3 (Recommended Security Controls for Federal Information Systems).<br><br>AWS maintains and provides security awareness training to all information system users supporting AWS. This annual security awareness training includes the following topics; The purpose for security and awareness training, The location of all AWS policies, AWS incident response procedures (including instructions on how to report internal and external security incidents).<br><br>AWS policies, procedures and relevant training programs are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP[sm] compliance | MS-4 | SOC1 (1.2)<br>SOC2 (S1.1, S1.2, S1.3, S2.2, S2.3, S2.4, S3.7 S3.8, S3.9, S4.2, S4.3)) | 5.1.1<br>5.1.2<br>6.1.1<br>8.1.3<br>8.2.2 | 3.1<br>8.5<br>12.1<br>12.2<br>12.3<br>12.6 | AT-1<br>AT-2<br>AT-3<br>AT-4<br>PL-1<br>PS-7 |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| MS.S-4.0 | Policies and Procedures | Provide in-depth training specific to the content handled by the facility | | | | | | |
| MS-4.1 | Policies and Procedures | Review and update security policies and procedures at least annually | | | | | | |
| MS.S-4.1 | Policies and Procedures | Provide training on the applications and processes surrounding encryption and key management for all individuals who handle encrypted content | | | | | | |
| MS-4.2 | Policies and Procedures | Require a sign-off from all company personnel (e.g., employees, temporary workers, interns) and third party workers (e.g., contractors, freelancers, temp agencies) for all policies, procedures, and/or client requirements and any updates | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| MS-4.3 | Policies and Procedures | Develop and regularly update a security awareness program and train company personnel and third party workers upon hire and annually thereafter on the security policies and procedures, addressing the following areas at a minimum:<br>• IT security policies and procedures<br>• Content/asset security and handling<br>• Security incident reporting and escalation<br>• Disciplinary measures | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| MS-5.0 | Incident Response | Establish a formal incident response plan that describes actions to be taken when a security incident is detected and reported | AWS has implemented a formal, documented incident response policy and program. The policy addresses purpose, scope, roles, responsibilities, and management commitment.<br><br>AWS utilizes a three-phased approach to manage incidents:<br>1. Activation and Notification Phase: Incidents for AWS begin with the detection of an event. This can come from several sources including:<br>a. Metrics and alarms - AWS maintains an exceptional situational awareness capability, most issues are rapidly detected from 24x7x365 monitoring and alarming of real time metrics and service dashboards. The majority of incidents are detected in this manner. AWS utilizes early indicator alarms to proactively identify issues that may ultimately impact Customers.<br>b. Trouble ticket entered by an AWS employee<br>c. Calls to the 24X7X365 technical support hotline.<br><br>If the event meets incident criteria, then the relevant on-call support engineer will start an engagement utilizing AWS Event Management Tool system to start the engagement and page relevant program resolvers (e.g. Security team). The resolvers will perform an analysis of the incident to determine if additional resolvers should be engaged and to determine the approximate root cause.<br><br>2. Recovery Phase - the relevant resolvers will perform break fix to address the incident. Once troubleshooting, break fix and affected components are addressed, the call leader will assign next steps in terms of follow-up documentation and follow-up actions and end the call engagement. | MS-5 | SOC 1 (8.2)<br>SOC 2 (S2.4, S3.5, S3.7, S3.9) | 13.1<br>13.1.1<br>13.2.2 | 12.9 | IR-1<br>IR-2<br>IR-4<br>IR-5<br>IR-6<br>IR-7<br>IR-8 |
| MS-5.1 | Incident Response | Identify the security incident response team who will be responsible for detecting, analyzing, and remediating security incidents | | | | | | |
| MS-5.2 | Incident Response | Establish a security incident reporting process for individuals to report detected incidents to the security incident response team | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| MS-5.3 | Incident Response | Communicate incidents promptly to clients whose content may have been leaked, stolen or otherwise compromised (e.g., missing client assets), and conduct a post-mortem meeting with management and client | 3. Reconstitution Phase - Once the relevant fix activities are complete the call leader will declare that the recovery phase is complete. Post mortem and deep root cause analysis of the incident will be assigned to the relevant team. The results of the post mortem will be reviewed by relevant senior management and relevant actions such as design changes etc. will be captured in a Correction of Errors (COE) document and tracked to completion.<br><br>In addition to the internal communication mechanisms detailed above, AWS has also implemented various methods of external communication to support its customer base and community. Mechanisms are in place to allow the customer support team to be notified of operational issues that impact the customer experience. A "Service Health Dashboard" is available and maintained by the customer support team to alert customers to any issues that may be of broad impact.<br><br>AWS incident management program reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP$^{sm}$ compliance | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| MS-6.0 | Workflow | Document a workflow that includes the tracking of content and authorization checkpoints throughout each process; include the following processes for both physical and digital content:<br>• Delivery<br>• Ingest<br>• Movement<br>• Storage<br>• Return to originator<br>• Removal from the site<br>• Destruction | Workflow documentation of Content (data) is the responsibility of AWS Customers as Customers retain ownership and control of their own guest operating systems, software, applications and data. | MS-6 | Not Applicable to AWS | Not Applicable to AWS | Not Applicable to AWS | Not Applicable to AWS |
| MS-6.1 | Workflow | Identify, implement, and assess the effectiveness of key controls to prevent, detect, and correct risks related to the content workflow | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| MS-7.0 | Segregation of Duties | Segregate duties within the content workflow, and implement and document compensating controls where segregation is not practical | Segregation of duties of Workflow of Content (data) is the responsibility of AWS Customers as Customers retain ownership and control of their own guest operating systems, software, applications and data.<br><br>Customers hosting digital assets and workflow on AWS can leverage AWS Identity and Access Management where appropriate to implement control requirements related to segregation of duties with regard to digital assets and content transfer. Customers can leverage AWS CloudTrail to assist with review and retention of audit logs where appropriate. | MS-7 | Not Applicable to AWS | Not Applicable to AWS | Not Applicable to AWS | Not Applicable to AWS |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| MS-8.0 | Background Checks | Perform background screening checks on all company personnel and third party workers | AWS conducts criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees commensurate with the employee's position and level of access to AWS facilities.<br><br>AWS background check program is reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP[sm] compliance | MS-8 | SOC 2 (S3.11) | 8.1.2 | 12.7 | PS-3 |
| MS-9.0 | Confidentiality Agreements | Require all company personnel and third party workers to sign a confidentiality agreement (e.g., non-disclosure) upon hire and annually thereafter, that includes requirements for handling and protecting content | Amazon Legal Counsel manages and periodically revises the Amazon Non-Disclosure Agreement (NDA) to reflect AWS business needs.<br><br>AWS usage of Non-Disclosure Agreements (NDA) is reviewed by independent external auditors during audits for our ISO 27001 and FedRAMP[sm] compliance | MS-9 | | 6.1.5<br>8.2.3<br>8.3.3 | | PL-4<br>PS-4<br>PS-6<br>PS-8<br>SA-9 |
| MS-9.1 | Confidentiality Agreements | Require all company personnel and third party workers to return all content and client information in their possession upon termination of their employment or contract | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| MS-10.0 | Third Party Use and Screening | Require all third party workers who handle content to sign confidentiality agreements (e.g., non-disclosure) upon engagement | As part of the on-boarding process, all personnel supporting AWS systems and devices sign a non-disclosure agreement prior to being granted access. Additionally, as part of orientation, personnel are required to read and accept the Acceptable Use Policy and the Amazon Code of Business Conduct and Ethics (Code of Conduct) Policy.<br><br>Personnel security requirements for third-party providers supporting AWS systems and devices are established in a Mutual Non-Disclosure Agreement between AWS' parent organization, Amazon.com, and the respective third-party provider. The Amazon Legal Counsel and the AWS Procurement team define AWS third party provider personnel security requirements in contract agreements with the third party provider. All persons working with AWS information must at a minimum, meet the screening process for pre-employment background checks and sign a Non-Disclosure Agreement (NDA) prior to being granted access to AWS information.<br><br>AWS Third Party requirements are reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP[sm] compliance. | MS-10 | | 6.1.5<br>6.2<br>6.2.3<br>10.2<br>11.1<br>11.2 | 12.8 | PL-4<br>PS-4<br>PS-6<br>PS-7<br>PS-8<br>SA-9 |
| MS.S-10.0 | Third Party Use and Screening | Communicate to clients the use of third-party storage providers for physical assets | | | | | | |
| MS-10.1 | Third Party Use and Screening | Include security requirements in third party contracts | | | | | | |
| MS.S-10.1 | Third Party Use and Screening | Require international (to/from U.S.) transportation companies to be "Customs-Trade Partnership Against Terrorism" (CTPAT) certified | | | | | | |
| MS-10.2 | Third Party Use and Screening | Implement a process to reclaim assets and remind third party workers of confidentiality agreements and contractual security requirements when terminating relationships | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| MS.S-10.2 | Third Party Use and Screening | Re-assess transportation and packaging vendors annually and when the vendor changes its location and/or provides additional services | | | | | | |
| MS-10.3 | Third Party Use and Screening | Require third party workers to be bonded and insured where appropriate (e.g., courier service) | | | | | | |
| MS.S-10.3 | Third Party Use and Screening | Review access to third-party content delivery systems and websites annually | | | | | | |
| MS-10.4 | Third Party Use and Screening | Restrict third party access to content/production areas unless required for their job function | | | | | | |
| MS.S-10.4 | Third Party Use and Screening | Incorporate security due diligence activities (e.g., security assessment, self-assessment questionnaire) as part of a selection and hiring process for third party workers who handle sensitive content | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| MS-10.5 | Third Party Use and Screening | Require third party companies to notify clients if they are on-boarding additional third party companies to handle content | | | | | | |
| PS-1.0 | Entry/Exit Points | Lock all entry/exit points at all times if the facility does not have a segregated access-controlled area beyond reception | AWS utilizes multi-factor authentication mechanisms for data center access as well as additional security mechanisms designed to ensure that only authorized individuals enter an AWS data center. Authorized individuals must use their badge on the card reader and enter their unique PIN to gain access to the facility and rooms for which they are authorized.<br><br>Physical access to data centers is enforced by AWS's electronic access control system, which is comprised of card readers and PIN pads for building and room ingress and card readers only for building and room egress. Enforcing the use of card readers for building and room egress provides anti-pass back functionality to help ensure that unauthorized individuals do not tailgate authorized Persons and get in without a badge.<br><br>In addition to the access control system, all entrances to AWS data centers, including the main entrance, the loading dock, and any roof doors/hatches, are secured with intrusion detection devices that sound alarms if the door is forced open or held open.<br><br>In addition to electronic mechanisms, AWS data centers utilize trained security guards 24x7, who are stationed in and around the building.<br><br>Access to data centers within the system boundary is granted on a need-to-know basis only, with all physical access requests being reviewed and approved by the | PS-1 | SOC 1 (5.5)<br>SOC 2 (S3.3, S3.4) | 9.1.1<br>9.1.2 | 9.1 | PE-3<br>PE-6 |
| PS.S-1.0 | Entry/Exit Points | Post security guards at all non-emergency entry/exit points | | | | | | |
| PS-1.1 | Entry/Exit Points | Control access to areas where content is handled by segregating the content area from other facility areas (e.g., administrative offices) | | | | | | |
| PS.S-1.1 | Entry/Exit Points | Lock and install alarms on all loading dock doors, and monitor loading dock doors while in use | | | | | | |
| PS.S-1.2 | Entry/Exit Points | Segregate the truck driver's entrance to prevent truck drivers from entering other areas of the facility | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS.S-1.3 | Entry/Exit Points | Implement a daily security patrol process with a randomized schedule and document the patrol results in a log | appropriate Area Access Manager (AAM).<br><br>AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP[sm] compliance. | | | | | |
| PS.S-1.4 | Entry/Exit Points | Document, investigate, and resolve all incidents detected during security guard shifts | | | | | | |
| PS-2.0 | Visitor Entry/Exit | Maintain a detailed visitors' log which includes the following:<br>• Name<br>• Company<br>• Time in/time out<br>• Person/people visited<br>• Signature of visitor<br>• Badge number assigned | AWS data centers are housed in nondescript facilities and are not open to the public. Physical access is strictly controlled both at the perimeter and at building ingress points. AWS only provides data center access and information to vendors, contractors, and visitors who have a legitimate business need for such privileges, such as emergency repairs. All visitors to data centers must be pre-authorized by the applicable Area Access Manager (AAM) and documented in AWS ticket management system. When they arrive at the data center, they must present identification and sign in before they are issued a visitor badge. They are continually escorted by authorized staff while in the data center.<br><br>AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP[sm] compliance. | PS-2 | SOC 1 (5.1)<br>SOC 2 (S3.3, S3.4) | 9.1.2 | 9.2<br>9.4 | PE-3<br>PE-7 |
| PS-2.1 | Visitor Entry/Exit | Assign an identification badge or sticker, which must be visible at all times, to each visitor and collect badges upon exit | | | | | | |
| PS-2.2 | Visitor Entry/Exit | Do not provide visitors with electronic access to content/production areas | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS-2.3 | Visitor Entry/Exit | Require visitors to be escorted by authorized employees while on-site, or in content/production areas at a minimum | | | | | | |
| PS-3.0 | Identification | Provide company personnel and long-term third party workers (e.g., janitorial) with photo identification that is validated and required to be visible at all times | AWS provides personnel with approved long term data center access an electronic access card with photographic identification.<br><br>AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP[sm] compliance. | PS-3 | SOC 1 (5.1)<br>SOC 2 (S3.3, S3.4) | 9.1.2 | 9.2<br>9.4 | PE-3 |
| PS-4.0 | Perimeter Security | Implement perimeter security controls that address risks that the facility may be exposed to as identified by the organization's risk assessment | Physical access to data centers is enforced by AWS's electronic access control system, which is comprised of card readers and PIN pads for building and room ingress and card readers only for building and room egress. Enforcing the use of card readers for building and room egress provides anti-pass back functionality to help ensure that unauthorized individuals do not tailgate authorized Persons and get in without a badge.<br><br>In addition to the access control system, all entrances to AWS data centers, including the main entrance, the loading dock, and any roof doors/hatches, are secured with intrusion detection devices that sound alarms if the door is forced open or held open.<br><br>In addition to electronic mechanisms, AWS data centers utilize trained security guards 24x7, who are stationed in and around the building. | PS-4 | SOC 1 (5.5)<br>SOC 2 (S3.3, S3.4) | 9.1.1 | 9.1 | PE-3 |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS.S-4.0 | Perimeter Security | Install additional perimeter safeguards (e.g., fences, vehicle barricades) to decrease the risk of unauthorized access onto the premises | Access to data centers within the system boundary is granted on a need-to-know basis only, with all physical access requests being reviewed and approved by the appropriate Area Access Manager (AAM).<br><br>AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP[sm] compliance. | | | | | |
| PS.S-4.1 | Perimeter Security | Lock perimeter gates at all times and dedicate an on-site employee to handle remote unlocking capabilities | | | | | | |
| PS.S-4.2 | Perimeter Security | Station a security guard at perimeter entrances and implement a process (e.g., electronic gate arm, parking permits) to allow vehicles into the facility campus | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS-5.0 | Alarms | Install a centralized, audible alarm system that covers all entry/exit points (including emergency exits), loading docks, fire escapes, and restricted areas (e.g., vault, server/machine room) | All entrances to AWS data centers, including the main entrance, the loading dock, and any roof doors/hatches, are secured with intrusion detection devices that sound alarms and create an alarm in AWS centralized physical security monitoring too if a door is forced open or held open.<br><br>In addition to electronic mechanisms, AWS data centers utilize trained security guards 24x7, who are stationed in and around the building. All alarms are investigated by a security guard with root cause documented for all incidents. All alarms are set to auto-escalate if response does not occur within SLA time.<br><br>Access to data centers within the system boundary is granted on a need-to-know basis only, with all physical access requests being reviewed and approved by the appropriate Area Access Manager (AAM).<br><br>AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP[sm] compliance. | PS-5 | SOC 1 (5.5)<br>SOC 2 (S3.3, S3.4) | 9.1 | 9.1 | PE-3<br>PE-6 |
| PS-5.1 | Alarms | Configure alarms to provide escalation notifications directly to the personnel in charge of security and/or be monitored by a central security group or third party | | | | | | |
| PS-5.2 | Alarms | Assign unique arm and disarm codes to each person that requires access to the alarm system and restrict access to all other personnel | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS-5.3 | Alarms | Review the list of users who can arm and disarm alarm systems annually | | | | | | |
| PS-5.4 | Alarms | Test the alarm system every 6 months | | | | | | |
| PS-5.5 | Alarms | Install and effectively position motion detectors in restricted areas (e.g., vault, server/machine room) and configure them to alert the appropriate security personnel and/or third-party | | | | | | |
| PS-5.6 | Alarms | Install door prop alarms for content/production areas to notify when sensitive entry/exit points are open for longer than a pre-determined period of time (e.g., 60 seconds) | | | | | | |
| PS-6.0 | Authorization | Document and implement a process to manage facility access and keep records of any changes to access rights | Physical access to data centers is enforced by AWS's electronic access control system, which is comprised of card readers and PIN pads for building and room ingress and card readers only for building and room egress. Enforcing the use of card readers for building and room egress provides anti-pass back functionality to help ensure that unauthorized individuals do not tailgate authorized Persons and get in without a badge. | PS-4 | SOC 1 (5.3, 5.5)<br>SOC 2 (S3.3, S3.4, S5.3) | 11.2<br>11.2.4 | 9.1 | PE-1<br>PE-2<br>PE-3<br>PE-4<br>PE-5 |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS.S-6.0 | Authorization | Review access to restricted areas (e.g., vault, safe) on a monthly basis and when the roles or employment status of any company personnel and/or third party workers change | In addition to the access control system, all entrances to AWS data centers, including the main entrance, the loading dock, and any roof doors/hatches, are secured with intrusion detection devices that sound alarms if the door is forced open or held open.<br><br>In addition to electronic mechanisms, AWS data centers utilize trained security guards 24x7, who are stationed in and around the building.<br><br>Access to data centers within the system boundary is granted on a need-to-know basis only, with all physical access requests being reviewed and approved by the appropriate Area Access Manager (AAM).<br><br>AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP[sm] compliance. | | | | | |
| PS-6.1 | Authorization | Restrict access to production systems to authorized personnel only | | | | | | |
| PS-6.2 | Authorization | Review access to restricted areas (e.g., vault, server/machine room) quarterly and when the roles or employment status of company personnel and/or third party workers are changed | | | | | | |
| PS-7.0 | Electronic Access | Implement electronic access throughout the facility to cover all entry/exit points and all areas where content is stored, transmitted, or processed | Physical access to data centers is enforced by AWS's electronic access control system, which is comprised of card readers and PIN pads for building and room ingress and card readers only for building and room egress. Enforcing the use of card readers for building and room egress provides anti-pass back functionality to help ensure that unauthorized individuals do not tailgate authorized Persons and get in without a badge. The ability to create and print a badge is systematically enforced and restricted to a core set of security personnel. All badges are activated for a finite time period requiring re-approval prior to extension of badge expiration date.<br><br>AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our | MS-9 | SOC 1 (5.3, 5.5)<br>SOC 2 (S3.3, S3.4, S5.3 | 9.1.2<br>9.1.3<br>11.2 | 9.1 | PE-2<br>PE-3<br>PE-7 |
| PS.S-7.0 | Electronic Access | Establish separate rooms for replication and for mastering | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS-7.1 | Electronic Access | Restrict electronic access system administration to appropriate personnel | SOC, PCI DSS, ISO 27001 and FedRAMP[sm] compliance. | | | | | |
| PS-7.2 | Electronic Access | Store blank card stock in a locked cabinet and ensure keycards remain disabled prior to being assigned to personnel | | | | | | |
| PS-7.3 | Electronic Access | Disable lost keycards in the system before issuing a new keycard | | | | | | |
| PS-7.4 | Electronic Access | Issue third party access cards with a set expiration date (e.g. 90 days) based on an approved timeframe | | | | | | |
| PS-8.0 | Keys | Limit the distribution of master keys to authorized personnel only (e.g., owner, facilities management) | Physical security processes and procedures, including procedures for managing facility Master keys are owned, managed and executed by AWS physical security staff.<br><br>AWS Physical Security Mechanisms are reviewed by | PS-8 | SOC 1 (5.5)<br>SOC 2 (S3.3, S3.4, S5.3 | 7.1.1<br>9.1.2<br>9.1.3 | 9.1 | PE-2<br>PE-3<br>CM-8 |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS-8.1 | Keys | Implement a check-in/check-out process to track and monitor the distribution of master keys | independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP[sm] compliance | | | | | |
| PS-8.2 | Keys | Use keys that can only be copied by a specific locksmith for exterior entry/exit points | | | | | | |
| PS-8.3 | Keys | Inventory master keys and keys to restricted areas, including facility entry/exit points, quarterly | | | | | | |
| PS-9.0 | Cameras | Install a CCTV system that records all facility entry/exit points and restricted areas | Physical access is controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems and other electronic means. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy. Images are retained for 90 days, unless limited to 30 days by legal or contractual obligations.<br><br>AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our | PS-9 | SOC 1 (5.4)<br>SOC 2 (S3.3) | 9.1.2<br>9.1.3<br>10.10.6 | 9.1 | PE-2<br>PE-3<br>PE-6 |
| PS.S-9.0 | Cameras | Review camera positioning, image quality, frame rate and retention daily | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS-9.1 | Cameras | Review camera positioning, image quality, lighting conditions, frame rate, and adequate retention of surveillance footage at least weekly | SOC, PCI DSS, ISO 27001 and FedRAMP[sm] compliance | | | | | |
| PS.S-9.1 | Cameras | Designate an employee or group of employees to monitor surveillance footage during operating hours and immediately investigate detected security incidents | | | | | | |
| PS-9.2 | Cameras | Restrict physical and logical access to the CCTV console and to CCTV equipment (e.g., DVRs) to personnel responsible for administering/monitoring the system | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS-9.3 | Cameras | Ensure that camera footage includes an accurate date and time-stamp | | | | | | |
| PS-10.0 | Logging and Monitoring | Log and review electronic access to restricted areas for suspicious events | Physical access is controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems and other electronic means.<br>All entrances to AWS data centers, including the main entrance, the loading dock, and any roof doors/hatches, are secured with intrusion detection devices that sound alarms and create an alarm in AWS centralized physical security monitoring too if a door is forced open or held open.<br><br>In addition to electronic mechanisms, AWS data centers utilize trained security guards 24x7, who are stationed in and around the building. All alarms are investigated by a security guard with root cause documented for all incidents. All alarms are set to auto-escalate if response does not occur within SLA time.<br><br>Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy. Images are retained for 90 days, unless limited to 30 days by legal or contractual obligations.<br><br>AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP[sm] compliance. | PS-10 | SOC 1 (5.3, 5.5)<br>SOC 2 (S3.3, S3.4, S5.3) | 10.10.2<br>10.10.3<br>13.1 | 9.1 | AU-3<br>AU-6<br>AU-9<br>AU-11 |
| PS.S-10.0 | Logging and Monitoring | Perform a weekly review of electronic access logs for the following areas, if applicable:<br>• Masters/stampers vault<br>• Pre-mastering<br>• Server/machine room<br>• Scrap room<br>• High-security cages | | | | | | |
| PS-10.1 | Logging and Monitoring | Investigate suspicious electronic access activities that are detected | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS-10.2 | Logging and Monitoring | Maintain an ongoing log of all confirmed electronic access incidents and include documentation of any follow-up activities that were taken | | | | | | |
| PS-10.3 | Logging and Monitoring | Retain CCTV surveillance footage and electronic access logs for at least 90 days, or the maximum time allowed by law, in a secure location | | | | | | |
| PS-11.0 | Searches | Inform company personnel and third party workers upon hire that bags and packages are subject to random searches and include a provision addressing searches in the facility policies | In alignment with AWS Physical Security Policies, AWS reserves the right to execute a search of bags and packages in the event of an issue.<br><br>AWS Physical Security Mechanisms are reviewed by independent external auditors during audits for our SOC, PCI DSS, ISO 27001 and FedRAMP[sm] compliance. | PS-11 | | 8.1.3 | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS.S-11.0 | Searches | Implement an exit search process that is applicable to all facility personnel and visitors, including:<br>• Removal of all outer coats, hats, and belts for inspection<br>• Removal of all pocket contents<br>• Performance of a self pat-down with the supervision of security<br>• Thorough inspection of all bags<br>• Inspection of laptops' CD/DVD tray<br>• Scanning of individuals with a handheld metal detector used within three inches of the individual searched | | | | | | |
| PS.S-11.1 | Searches | Prohibit personnel from entering/exiting the facility with digital recording devices (e.g., USB thumb drives, digital cameras, cell phones) and include the search of these devices as part of the exit search procedure | | | | | | |
| PS.S-11.2 | Searches | Enforce the use of transparent plastic bags and food containers for any food brought into production areas | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS.S-11.3 | Searches | Implement a dress code policy that prohibits the use of oversized clothing (e.g., baggy pants, oversized hooded sweatshirts) | | | | | | |
| PS.S-11.4 | Searches | Use numbered, tamper-evident stickers/holograms to identify authorized devices that can be taken in and out of the facility | | | | | | |
| PS.S-11.5 | Searches | Implement a process to test the exit search procedure | | | | | | |
| PS.S-11.6 | Searches | Perform a random vehicle search process when exiting the facility parking lot | | | | | | |
| PS.S-11.7 | Searches | Segregate replication lines that process highly sensitive content and perform searches upon exiting segregated areas | | | | | | |
| PS.S-11.8 | Searches | Implement additional controls to monitor security guard activity | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS-12.0 | Inventory Tracking | Implement a content asset management system to provide detailed tracking of physical assets (i.e., client and newly created) | Content Asset Management is owned, implemented and operated by AWS Customers. It is the responsibility of Customers to implement inventory tracking of their physical assets.<br><br>For AWS Data Center Environments, all new information system components, which include, but are not limited to, servers, racks, network devices, hard drives, system hardware components, and building materials that are shipped to and received by data centers require prior authorization by and notification to the Data Center Manager. Items are delivered to the loading dock of each AWS Data Center and are inspected for any damages or tampering with the packaging and signed for by a full-time employee of AWS. Upon shipment arrival, items are scanned and captured within the AWS Asset management system and device inventory tracking system.<br><br>Once items are received, they are placed in an equipment storage room within the data center that requires the swipe badge and PIN combination for access until they are installed on the data center floor. Prior to exiting the data center, items are scanned, tracked, and sanitized before authorization to leave the data center.<br><br>AWS Asset Management processes and procedures are reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP[sm] compliance. | PS-12 | | 7.1<br>7.1.1<br>10.10.3<br>10.10.6<br>15.1.3 | 9.6<br>9.7 | AU-9<br>AU-11<br>CM-8<br>MP-3 |
| PS.S-12.0 | Inventory Tracking | Use automated notification for assets that have been out of the vault for extended periods of time | | | | | | |
| PS-12.1 | Inventory Tracking | Barcode client assets and created media (e.g., tapes, hard drives) upon receipt and store assets in the vault when not in use | | | | | | |
| PS.S-12.1 | Inventory Tracking | Lock up and log assets that are delayed or returned if shipments could not be delivered on time | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS-12.2 | Inventory Tracking | Retain asset movement transaction logs for at least 90 days | | | | | | |
| PS-12.3 | Inventory Tracking | Review logs from content asset management system and investigate anomalies | | | | | | |
| PS-12.4 | Inventory Tracking | Use studio AKAs (“aliases”) when applicable in asset tracking systems and on any physical assets | | | | | | |
| PS-13.0 | Inventory Counts | Perform a quarterly inventory count of each client's pre-release project(s), reconcile against asset management records, and immediately communicate variances to clients | Customers retain the control and responsibility of their data and associated media assets. It is the responsibility of the customer to implement inventory tracking and monitoring of their physical assets.<br><br>AWS Asset Management system and device inventory tracking systems maintain systematic inventory of AWS Data Center information system components. Audits of inventory occur on a regular basis and are | PS-13 | | 7.1.1<br>10.1.3 | | AU-6<br>AC-5<br>IR-4<br>IR-5 |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS.S-13.0 | Inventory Counts | Perform a weekly inventory count of each client's pre-release project(s), reconcile against asset management records, and immediately communicate variances to clients | reviewed by an independent auditor as a part of our FedRAMP[sm] compliance program.<br><br>AWS Asset Management processes and procedures are reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP[sm] compliance. | | | | | |
| PS-13.1 | Inventory Counts | Segregate duties between the vault staff and individuals who are responsible for performing inventory counts | | | | | | |
| PS.S-13.1 | Inventory Counts | Monitor film elements (e.g., negatives, unprocessed film) constantly throughout the workflow process | | | | | | |
| PS-13.2 | Inventory Counts | Implement and review a daily aging report to identify highly sensitive assets that are checked out from the vault and not checked back in | | | | | | |
| PS-14.0 | Blank Media/ Raw Stock Tracking | Tag (e.g., barcode, assign unique identifier) blank stock/raw stock per unit when received | AWS customers retain control and ownership of their data and media assets. It is the responsibility of the Studio / Processing facility to manage security of media stock. | PS-14 | | 7.1.1<br>10.7.1 | | MP-4<br>MP-2<br>PE-2<br>PE-3 |
| PS.S-14.0 | Blank Media/ Raw Stock Tracking | Establish a process to track consumption of raw materials (e.g., polycarbonate) monthly | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS-14.1 | Blank Media/ Raw Stock Tracking | Store blank media/raw stock in a secured location | | | | | | |
| PS-15.0 | Client Assets | Restrict access to finished client assets to personnel responsible for tracking and managing assets | It is the responsibility of those individuals that Screen / manage physical copies of finished assets to ensure that adequate physical security is implemented.<br><br>As documented in MPAA PS-1 - PS-14 AWS operates a Physical Security Program and Asset Management Program throughout all of our data centers that is regularly reviewed and assessed by independent third party auditors as a part of our continued SOC, PCI DSS, ISO 27001 and FedRAMP[sm] compliance program. | PS-15 | SOC 1 (5.3, 5.5)<br>SOC 2 (S3.3, S3.4, S5.3) | 7.1.1<br>9.1.2<br>10.7.1 | 9.1<br>9.6<br>9.7 | MP-2<br>MP-4<br>PE-2<br>PE-3 |
| PS.S-15.0 | Client Assets | Require two company personnel with separate access cards to unlock highly sensitive areas (e.g., safe, high-security cage) after-hours | | | | | | |
| PS-15.1 | Client Assets | Store client assets in a restricted and secure area (e.g., vault, safe) | | | | | | |
| PS.S-15.1 | Client Assets | Use an access-controlled cage for the staging area and monitor the area with surveillance cameras | | | | | | |
| PS.S-15.2 | Client Assets | Use a locked fireproof safe to store undelivered packages that are kept at the facility overnight | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS.S-15.3 | Client Assets | Implement a dedicated, secure area (e.g., security cage, secure room) for the storage of undelivered screeners that is locked, access-controlled, and monitored with surveillance cameras and/or security guards | | | | | | |
| PS-16.0 | Disposals | Require that rejected, damaged, and obsolete stock are erased, degaussed, shredded, or physically destroyed before disposal (e.g., DVD shredding, hard drive destruction) and update asset management records to reflect destruction | When an AWS storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned storage devices are degaussed and physically destroyed in accordance with industry-standard practices<br><br>AWS storage device disposal process is regularly reviewed and assessed by independent third party auditors as a part of our continued ISO 27001 and FedRAMP[sm] compliance program. | PS-16 | | 9.2.6<br>10.7.2 | 9.10 | MP-6 |
| PS.S-16.0 | Disposals | Implement a process that requires security personnel to monitor and record the scrapping process if scrap is destroyed | | | | | | |
| PS-16.1 | Disposals | Store elements targeted for recycling/destruction in a secure location/container to prevent the copying and reuse of assets prior to disposal | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS.S-16.1 | Disposals | Conduct periodic security training for all company personnel and third party workers to educate on asset disposal and destruction processes (e.g., placing assets into designated containers) | | | | | | |
| PS-16.2 | Disposals | Maintain a log of asset disposal for at least 12 months | | | | | | |
| PS.S-16.2 | Disposals | Scratch discs before placing them into the scrap bin | | | | | | |
| PS-16.3 | Disposals | Require third-party companies who handle destruction of content to provide a certificate of destruction for each completed job | | | | | | |
| PS.S-16.3 | Disposals | Use automation to transfer rejected discs from replication machines directly into scrap bins (no machine operator handling) | | | | | | |
| PS.S-16.4 | Disposals | Prohibit the use of third party companies for the destruction of DCDM drives or pre-released content | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS-17.0 | Shipping | Require the facility to file a valid work/shipping order to authorize asset shipments out of the facility | For AWS Data Center Environments, all new information system components, which include, but are not limited to, servers, racks, network devices, hard drives, system hardware components, and building materials that are shipped to and received by data centers require prior authorization by and notification to the Data Center Manager. Items are delivered to the loading dock of each AWS Data Center and are inspected for any damages or tampering with the packaging and signed for by a full-time employee of AWS. Upon shipment arrival, items are scanned and captured within the AWS Asset management system and device inventory tracking system.<br><br>AWS Asset Management processes and procedures are reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP[sm] compliance. | PS-17 | | 9.1.2<br>10.8.2<br>10.8.3 | 9.6<br>9.7 | MP-5<br>AU-11<br>PE-16 |
| PS.S-17.0 | Shipping | Document and retain a separate log for truck driver information | | | | | | |
| PS-17.1 | Shipping | Track and log asset shipping details; at a minimum, include the following:<br>• Time of shipment<br>• Sender name and signature<br>• Recipient name<br>• Address of destination<br>• Tracking number from courier<br>• Reference to the corresponding work order | | | | | | |
| PS.S-17.1 | Shipping | Require personnel picking up package(s) to verify the count the shipping document and obtain a signature from the shipping point | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS-17.2 | Shipping | Validate assets leaving the facility against a valid work/shipping order | | | | | | |
| PS.S-17.2 | Shipping | Observe and monitor the packing and sealing of trailers when shipping occurs on-site | | | | | | |
| PS-17.3 | Shipping | Secure assets that are waiting to be picked up | | | | | | |
| PS.S-17.3 | Shipping | Implement a formal process to record, monitor, and review travel times, routes, and delivery times for shipments between facilities | | | | | | |
| PS-17.4 | Shipping | Prohibit couriers and delivery personnel from entering content/production areas of the facility | | | | | | |
| PS.S-17.4 | Shipping | Do not allow film elements to leave the facility other than through shipping, except with a signed authorization pass | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS.S-17.5 | Shipping | Ship prints for pre-theatrical screenings in segments (e.g., odd versus even reels) | | | | | | |
| PS-18.0 | Receiving | Inspect delivered content upon receipt and compare to shipping documents (e.g., packing slip, manifest log) | Once new information system components are received in the AWS Data Centers, they are placed in an equipment storage room within the data center that requires the swipe badge and PIN combination for access until they are installed on the data center floor. Prior to exiting the data center, items are scanned, tracked, and sanitized before authorization to leave the data center.<br><br>AWS Asset Management processes and procedures are reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP[sm] compliance. | PS-18 | | 7.1<br>7.2<br>10.8.2<br>10.8.3 | 9.6<br>9.7 | MP-3<br>MP-4<br>PE-16 |
| PS-18.1 | Receiving | Maintain a receiving log to be filled out by designated personnel upon receipt of deliveries | | | | | | |
| PS-18.2 | Receiving | Perform the following actions immediately:<br>• Tag (e.g., barcode, assign unique identifier) received assets,<br>• Input the asset into the asset management system<br>• Move the asset to the restricted area (e.g., vault, safe) | | | | | | |
| PS-18.3 | Receiving | Implement a secure method (e.g., secure drop box) for receiving overnight deliveries | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS-19.0 | Labeling | Prohibit the use of title information, including AKAs ("aliases"), on the outside of packages | AWS Asset labels are customer agnostic and are utilized to maintain inventory of hardware within the AWS Asset Management Tool. Within AWS Data Centers hardware is not physically associated with a customer or the data stored on the hardware. All customer data, regardless of source is considered to be Critical, in turn, all media is treated as sensitive.<br><br>AWS Asset Management processes and procedures are reviewed by independent external auditors during audits for our PCI DSS, ISO 27001 and FedRAMP[sm] compliance. | PS-19 | | 7.2 | 9.6<br>9.7 | MP-3 |
| PS-20.0 | Packaging | Ship all assets in closed/sealed containers, and use locked containers depending on asset value | Packaging of physical finished media assets are the responsibility of the relevant distributing body (such as companies involved with distribution, DVD Creation, Post-production etc.). | PS-20 | | 10.8.3 | | MP-5 |
| PS.S-20.0 | Packaging | Apply shrink wrapping to all shipments, and inspect packaging before final shipment to ensure that it is adequately wrapped | | | | | | |
| PS-20.1 | Packaging | Implement at least one of the following controls:<br>• Tamper-evident tape<br>• Tamper-evident packaging<br>• Tamper-evident seals in the form of holograms<br>• Secure containers (e.g., Pelican case with a combination lock) | | | | | | |
| PS-21.0 | Transport Vehicles | Lock automobiles and trucks at all times, and do not place packages in visible auto/truck areas | Transport of physical finished media assets (such as DVD's) are the responsibility of the relevant distributing body (such as companies involved with distribution, DVD Creation, Post-production etc.). | PS-21 | | | | MP-5 |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| PS.S-21.0 | Transport Vehicles | Include the following security features in transportation vehicles (e.g., trailers):<br>• Segregation from driver cabin<br>• Ability to lock and seal cargo area doors<br>• GPS for high-security shipments | | | | | | |
| PS.S-21.1 | Transport Vehicles | Apply numbered seals on cargo doors for shipments of highly sensitive titles | | | | | | |
| PS.S-21.2 | Transport Vehicles | Require security escorts be used for delivery of highly sensitive content in high-risk areas | | | | | | |
| DS-1.0 | WAN | Segment WAN(s) by using stateful inspection firewalls with Access Control Lists that prevent unauthorized access to any internal network | Boundary protection devices that employ rule sets, access control lists (ACL), and configurations enforce the flow of information between network fabrics. Several network fabrics exist at Amazon, each separated by devices that control the flow of information between fabrics. The flow of information between fabrics is established by approved authorizations, which exist as access control lists (ACL) which reside on these devices. These devices control the flow of information between fabrics as mandated by these ACLs. ACLs are defined, approved by appropriate personnel, managed and deployed using AWS ACL-manage tool. | DS-1 | SOC 1(3.2, 3.3, 3.4, 3.7, 3.9, 3.10, 3.14, 3.15, 3.16)<br>SOC 2(S.3.2, S3.4, S.3.5, S4.1, S.4.2, S4.3,S3.12) | 11.1<br>11.4 | 1.1<br>1.2<br>1.3<br>1.4<br>2.2<br>6.6<br>8.5<br>11.2 | AC-2<br>AC-3<br>CM-7 |
| DS-1.1 | WAN | Develop a process to review firewall Access Control Lists (ACLs) to confirm configuration settings are appropriate and required by the business every 6 months | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-1.2 | WAN | Deny all protocols by default and enable only specific permitted secure protocols on the WAN | Amazon's Information Security team approves these ACLs. Approved firewall rule sets and access control lists between network fabrics restrict the flow of information to specific information system services. Access control lists and rule sets are reviewed and approved, and are automatically pushed to boundary protection devices on a periodic basis (at least every 24 hours) to ensure rule-sets and access control lists are up-to-date.<br><br>AWS Network Management is regularly reviewed by independent third party auditors as a part of AWS ongoing compliance with SOC, PCI DSS, ISO 27001 and FedRAMP[sm].<br><br>AWS implements least privilege throughout its infrastructure components. AWS prohibits all ports and protocols that do not have a specific business purpose. AWS follows a rigorous approach to minimal implementation of only those features and functions that are essential to use of the device. Network scanning is performed and any unnecessary ports or protocols in use are corrected.<br><br>Regular internal and external vulnerability scans are performed on the host operating system, web application and databases in the AWS environment utilizing a variety of tools. Vulnerability scanning and remediation practices are regularly reviewed as a part of AWS continued compliance with PCI DSS and FedRAMP[sm]. | | | | | |
| DS-1.3 | WAN | Place externally accessible servers (e.g., secure FTP server, web servers) within the DMZ | | | | | | |
| DS-1.4 | WAN | Implement a process to patch network infrastructure devices (e.g., firewalls, routers, switches, etc.) regularly | | | | | | |
| DS-1.5 | WAN | Harden network infrastructure devices based on security configuration standards | | | | | | |
| DS-1.6 | WAN | Do not allow remote access to WAN network infrastructure devices (e.g., firewall, router) that control access to content | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-1.7 | WAN | Secure backups of network infrastructure devices to a centrally secured server on the internal network | | | | | | |
| DS-1.8 | WAN | Perform an annual vulnerability scan on hosts that are externally accessible and remediate issues | | | | | | |
| DS-1.9 | WAN | Allow only authorized personnel to request the establishment of a connection with the telecom service provider | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-2.0 | Internet | Prohibit Internet access on systems (desktops/ servers) that process or store digital content | Boundary protection devices are configured in a deny-all mode which denies<br>Boundary protection devices that employ rule sets, access control lists (ACL), and configurations enforce the flow of information between network fabrics. These devices are configured in deny-all mode, requiring an approved firewall set to allow for connectivity. Refer to DS-2.0 for additional information on Management of AWS Network Firewalls.<br><br>There is no inherent e-mail capability on AWS Assets and port 25 is not utilized. A Customer (e.g. studio, processing facility etc.) can utilize a system to host e-mail capabilities, however in that case it is the Customer's responsibility to employ the appropriate levels of spam and malware protection at e-mail entry and exit points and update spam and malware definitions when new releases are made available.<br><br>Amazon assets (e.g. laptops) are configured with anti-virus software that includes e-mail filtering and malware detection.<br><br>AWS Network Firewall management and Amazon's anti-virus program are reviewed by independent third party auditors as a part of AWS ongoing compliance with SOC, PCI DSS, ISO 27001 and FedRAMP[sm]. | DS-2 | SOC 1(3.2, 3.3, 3.4, 3.7, 3.9, 3.10, 3.14, 3.15, 3.16)<br>SOC 2(S.3.2, S3.4, S.3.5, S4.1, S.4.2, S4.3,S3.12) | 7.1.3<br>11.2.2 | 1.1<br>1.2<br>1.3<br>1.4<br>2.2<br>5.1<br>6.6<br>8.5<br>11.2 | CA-3<br>PL-4 |
| DS-2.1 | Internet | Implement e-mail filtering software or appliances that block the following from non-production networks:<br>• Potential phishing e-mails<br>• Prohibited file attachments (e.g., Visual Basic scripts, executables, etc.)<br>• File size restrictions limited to 10 MB | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-2.2 | Internet | Implement web filtering software or appliances that restrict access to websites known for peer-to-peer file trading, viruses, hacking or other malicious sites | | | | | | |
| DS-3.0 | LAN | Isolate the content/production network from non-production networks (e.g., office network, DMZ, etc.) by means of physical or logical network segmentation | AWS provides customers the ability to segment and manage networks but is not responsible for the implementation and operation of these segmented environments. | DS-3 | | 11.2<br>11.4.2<br>11.4.4<br>10.6.2<br>10.10 | | AC-6<br>AC-17<br>CM-7<br>SI-4 |
| DS-3.1 | LAN | Restrict access to the content/production systems to authorized personnel | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-3.2 | LAN | Restrict remote access to the content/production network to only approved personnel who require access to perform their job responsibilities | | | | | | |
| DS-3.3 | LAN | Disable all unused switch ports on the content/production network to prevent packet sniffing by unauthorized devices | | | | | | |
| DS-3.4 | LAN | Restrict the use of non-switched devices such as hubs and repeaters on the content/production network | | | | | | |
| DS-3.5 | LAN | Prohibit dual-homed networking (network bridging) on computer systems within the content/production network | | | | | | |
| DS-3.6 | LAN | Implement a network-based intrusion detection or prevention system on the content/production network | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-4.0 | Wireless | Prohibit wireless networking and the use of wireless devices on the production/content network | There is no inherent wireless capability on AWS Assets.<br><br>Amazon assets (e.g. laptops) wireless capabilities are implemented and operated in alignment with industry standard secure wireless configuration standards. Amazon continuously monitors wireless networks in order to detect rouge devices.<br><br>AWS management of Wireless networks is reviewed | DS-4 | | 10.6.1<br>12.6 | 11.1 | AC-18<br>SI-4 |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-4.1 | Wireless | Configure non-production wireless networks (e.g., administrative and guest) with the following security controls:<br>• Disable WEP<br>• Enable AES encryption<br>• Segregate "guest" networks from the company's other networks | by independent third party auditors as a part of AWS ongoing compliance with PCI DSS, ISO 27001 and FedRAMP[sm]. | | | | | |
| DS-4.2 | Wireless | Implement a process to scan for rogue wireless access points annually | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-5.0 | I/O Device Security | Designate specific systems to be used for content input/output (I/O) | AWS prevents access to system output devices to only authorized persons. Access to obtain authorization requires the submission of an electronic request, providing a business case for access, and obtaining documented approval of that authorization by an Authorized Approver. AWS Access Management procedures are independently reviewed by a third party auditor as a part of continued compliance with SOC, PCI-DSS, ISO 27001 and FedRAMP[sm].<br><br>Personal electronic devices and removable media are prohibited from connecting to AWS information systems. | DS-5 | SOC 1 (2.1, 5.1)<br>SOC 2 (S.3.2, S3.3, S.3.4) | 10.7.1<br>10.10.2 | 7.1<br>8.2 | MP-2<br>AC-19<br>PE-5 |
| DS-5.1 | I/O Device Security | Block input/output (I/O) devices (e.g., USB, FireWire, e-SATA, SCSI, etc.) on all systems that handle or store content, with the exception of systems used for content I/O | | | | | | |
| DS-5.2 | I/O Device Security | Restrict the installation and/or use of media burners (e.g., DVD, Blu-ray, CD burners) and other devices with output capabilities to specific I/O systems used for outputting content to physical media | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-6.0 | System Security | Install anti-virus software on all workstations and servers | Within the AWS environment, a configuration management tool used to manage deployable software in packages, package groups, and environments. A package is a collection of related files, such as software, content, etc., that are tightly coupled. A package group is a set of packages that are often deployed together. An environment is the combination of a set of packages and package groups which are deployed to a set of host classes (hosts or servers that serve the same function). An environment represents the complete set of packages required for a server to fulfill a particular function.<br><br>AWS maintains the baseline OS distribution used on hosts. All unneeded ports, protocols and services are disabled in the base builds. Service teams use the build tools to add only approved software packages necessary for the servers function per the configuration baselines maintained in the tools.<br><br>Servers are regularly scanned and any unnecessary ports or protocols in use are corrected using the flaw remediation process. Deployed software undergoes recurring penetration testing performed by carefully selected industry experts. Remediation of the penetration testing exercise is also incorporated into the baseline through the flaw remediation process.<br><br>Amazon Information Security and AWS Security teams subscribe to newsfeeds for applicable vendor flaws from Secunia and TELUS Security Labs. Amazon Information Security proactively monitors vendor's websites and other relevant outlets for new patches. Prior to implementation Patches are evaluated for security and operational impact and applied in timely manner based upon assessment. | DS-4 | | 10.4.1<br>10.1.3<br>10.8.2<br>11.3.2<br>11.4.3<br>11.4.4 | | SI-3<br>SI-2<br>RA-5<br>AC-5<br>SC-2<br>PE-3<br>MA-4<br>PE-5<br>SA-7<br>SA-6 |
| DS-6.1 | System Security | Update anti-virus definitions daily | | | | | | |
| DS-6.2 | System Security | Scan file-based content for viruses prior to ingest onto the content/production network | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-6.3 | System Security | Performing virus scans as follows:<br>• Enable regular full system virus scanning on all workstations<br>• Enable full system virus scans for servers, where applicable (e.g., non-SAN systems) | Amazon assets (e.g. laptops) are configured with anti-virus software that includes e-mail filtering and malware detection.<br><br>AWS Configuration Management and Flaw Remediation Process are all reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP[sm]. | | | | | |
| DS-6.4 | System Security | Implement a process to regularly update systems (e.g., file transfer systems, operating systems, databases, applications, network devices) with patches/updates that remediate security vulnerabilities | | | | | | |
| DS-6.5 | System Security | Prohibit users from being Administrators on their own workstations | | | | | | |
| DS-6.6 | System Security | Use cable locks on portable computing devices that handle content (e.g., laptops, tablets, towers) when they are left unattended | | | | | | |
| DS-6.7 | System Security | Install remote-kill software on all portable computing devices that handle content to allow remote wiping of hard drives and other storage devices | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-6.8 | System Security | Restrict software installation privileges to approved users | | | | | | |
| DS-6.9 | System Security | Implement security baselines and standards to configure systems (e.g., laptops, workstations, servers) that are set up internally | | | | | | |
| DS-6.10 | System Security | Unnecessary services and applications should be uninstalled from content transfer servers | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-7.0 | Account Management | Establish and implement an account management process for administrator, user, and service accounts for all information systems and applications that handle content | AWS has a formal access control policy that is reviewed and updated on an annual basis (or when any major change to the system occurs that impacts the policy). The policy addresses purpose, scope, roles, responsibilities and management commitment.<br><br>AWS employs the concept of least privilege, allowing only the necessary access for users to accomplish their job function. When user accounts are created, user accounts are created to have minimal access. Access above these least privileges requires appropriate authorization.<br><br>Authorized users of AWS systems and devices are provided access privileges via group membership specific to the authorized individuals job function and role. Conditions for group membership are established and verified by group owners. User, group, and system accounts all have unique identifiers and are not reused. Guest/anonymous and temporary accounts are not used and are not allowed on devices.<br><br>User accounts are reviewed at least quarterly. On a quarterly basis, all group owners review and remove, as needed, any users who no longer require group membership. This review is initiated by a systematic notification sent to the group owner by the AWS Account Management Tool, which notifies the group owner to perform a baseline of the group. A baseline is a full re-evaluation of permissions by the group owner. If the baseline isn't completed by the deadline, | DS-7 | SOC 1 (2.1, 2.2)<br>SOC 2 (S.3.2, S.3.4) | 10.1.3<br>10.10.4<br>11.2<br>11.2.1<br>11.2.2<br>11.2.4 | 7.1<br>8.1<br>8.2 | AC-2<br>AC-5<br>AC-6<br>AU-2<br>AU-12<br>IA-4<br>PS-4<br>PS-5<br>PE-2 |
| DS-7.1 | Account Management | Maintain traceable evidence of the account management activities (e.g., approval e-mails, change request forms) | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-7.2 | Account Management | Assign unique credentials on a need-to-know basis using the principles of least privilege | all group members are removed. User accounts are automatically disabled systematically after 90 days of inactivity.<br><br>AWS have identified auditable event categories across systems and devices within the AWS system. Service teams configure the auditing features to record continuously the security-related events in accordance with requirements. The log storage system is designed to provide a highly scalable, highly available service that automatically increases capacity as the ensuing need for log storage grows.<br><br>AWS Access Management procedures are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP[sm]. | | | | | |
| DS-7.3 | Account Management | Rename the default administrator accounts and limit the use of these accounts to special situations that require these credentials (e.g., operating system updates, patch installations, software updates) | | | | | | |
| DS-7.4 | Account Management | Segregate duties to ensure that individuals responsible for assigning access to information systems are not themselves end users of those systems (i.e., personnel should not be able to assign access to themselves) | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-7.5 | Account Management | Monitor and audit administrator and service account activities | | | | | | |
| DS-7.6 | Account Management | Implement a process to review user access for all information systems that handle content and remove any user accounts that no longer require access quarterly | | | | | | |
| DS-7.7 | Account Management | Review user access to content on a per-project basis | | | | | | |
| DS-7.8 | Account Management | Disable or remove local accounts on systems that handle content where technically feasible | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-8.0 | Authentication | Enforce the use of unique usernames and passwords to access information systems | Unique user identifiers are created as part of the onboarding workflow process in the AWS human resources management system. The device provisioning process helps ensure unique identifiers for devices. Both processes include manager approval to establish the user account or device. Initial authenticators are delivered to user's in-person and to devices as part of the provisioning process. Internal users can associate SSH public keys with their account. System account authenticators are provided to the requestor as part of the account creation process after the identity of the requestor is verified. Minimum strength of authenticators is defined by AWS including password length, requires complex passwords and password age requirements and content along with SSH key minimum bit length.<br><br>AWS Password policy and implementation is reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP[sm]. | DS-8 | SOC 1 (2.5)<br>SOC 2 (S.3.2, S.3.4) | 11.2.1<br>11.2.3<br>11.4.2<br>11.5.2 | 8.4<br>8.5 | IA-2<br>IA-4<br>IA-5<br>AC-7<br>AC-11<br>AC-17 |
| DS-8.1 | Authentication | Enforce a strong password policy for gaining access to information systems | | | | | | |
| DS-8.2 | Authentication | Implement two-factor authentication (e.g., username/password and hard token) for remote access (e.g., VPN) to the networks. | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-8.3 | Authentication | Implement password-protected screensavers or screen-lock software for servers and workstations | | | | | | |
| DS-9.0 | Logging and Monitoring | Implement real-time logging and reporting systems to record and report security events; gather the following information at a minimum:<br>• When (time stamp)<br>• Where (source)<br>• Who (user name)<br>• What (content) | AWS has identified auditable event categories across systems and devices within the AWS system. Service teams configure the auditing features to record continuously the security-related events in accordance with requirements. The log storage system is designed to provide a highly scalable, highly available service that automatically increases capacity as the ensuing need for log storage grows. Audit records contain a set of data elements in order to support necessary analysis requirements. In addition, audit records are available for AWS Security team or other appropriate teams to perform inspection or analysis on demand, and in response to security-related or business-impacting events.<br><br>Designated personnel on AWS teams receive automated alerts in the event of an audit processing failure. Audit processing failures include, for example, software/hardware errors. When alerted, on-call personnel issue a trouble ticket and track the event until it is resolved. | DS-9 | SOC 1 (3.6) | 10.1<br>10.10.2<br>10.10.5 | 10.1<br>10.2<br>10.3 | AU-1<br>AU-2<br>AU-3<br>AU-6<br>SI-4 |
| DS.S-9.0 | Logging and Monitoring | Implement logging mechanisms on all systems used for:<br>• Key generation<br>• Key management<br>• Vendor certificate management | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-9.1 | Logging and Monitoring | Configure logging systems to send automatic notifications when security events are detected in order to facilitate active response to incidents | AWS logging and monitoring processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP[sm]. | | | | | |
| DS-9.2 | Logging and Monitoring | Investigate any unusual activity reported by the logging and reporting systems | | | | | | |
| DS-9.3 | Logging and Monitoring | Review logs weekly | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-9.4 | Logging and Monitoring | Enable logging of internal and external content movement and transfers and include the following information at a minimum:<br>• Username<br>• Timestamp<br>• File name<br>• Source IP address<br>• Destination IP address<br>• Event (e.g., download, view) | | | | | | |
| DS-9.5 | Logging and Monitoring | Retain logs for at least 6 months | | | | | | |
| DS-9.6 | Logging and Monitoring | Restrict log access to appropriate personnel | | | | | | |
| DS-9.7 | Logging and Monitoring | Send automatic notifications to the production coordinator(s) upon outbound content transmission | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-10.0 | Security Techniques | Ensure that security techniques (e.g., spoiling, invisible/visible watermarking) are available for use and are applied when instructed | AWS provides customers the ability to use their own encryption mechanism for nearly all services including S3, EBS and EC2. VPC sessions are also encrypted.<br><br>Internally, AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. AWS produces, controls and distributes symmetric cryptographic keys using NIST approved key management technology and processes in the AWS information system. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute: AWS credentials needed on hosts, RSA public/private keys and X.509 Certifications.<br><br>AWS cryptographic processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP[sm]. | DS-10 | | 7.2.2<br>12.3.1<br>12.3.2 | 3.4.1 | IA-5<br>SC-9<br>SC-12<br>SC-13 |
| DS.S-10.0 | Advanced Security Techniques | Implement a process for key management that addresses the following:<br>• Approval and revocation of trusted devices<br>• Generation, renewal, and revocation of content keys<br>• Internal and external distribution of content keys | | | | | | |
| DS-10.1 | Security Techniques | Encrypt content on hard drives using a minimum of AES 128-bit encryption by either:<br>• File-based encryption: (i.e., encrypting the content itself)<br>• Drive-based encryption: (i.e., encrypting the hard drive) | | | | | | |
| DS.S-10.1 | Advanced Security Techniques | Confirm that devices on the Trusted Devices List (TDL) are appropriate based on rights owners' approval | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-10.2 | Security Techniques | Send decryption keys or passwords using an out-of-band communication protocol (i.e., not on the same storage media as the content itself) | | | | | | |
| DS.S-10.2 | Advanced Security Techniques | Confirm the validity of content keys and ensure that expiration dates conform with client instructions | | | | | | |
| DS-11.0 | Transfer Tools | Implement transfer tools that use access controls, a minimum of AES 128-bit encryption and strong authentication for content transfer sessions | AWS provides customers the ability to use their own encryption mechanism for nearly all services including S3, EBS and EC2. VPC sessions are also encrypted.<br><br>For AWS connections, FIPS-approved hashes are available. AWS utilizes cryptographic modules for user authentication through the following access methods; API Endpoints, VPC IPSEC VPN, IAM, MFA Hardware Token, SSH. | DS-11 | SOC 1 (4.1, 4.2, 4.3)<br>SOC 2 (S.3.6) | 12.3.1 | 3.4.1 | IA-5<br>SC-13 |
| DS-11.1 | Transfer Tools | Implement an exception process, where client prior approval must be obtained in writing, to address situations where encrypted transfer tools are not used | | | | | | |
| DS-12.0 | Transfer Device Methodology | Implement and use dedicated systems for content transfers | AWS provides customers the ability to segment and manage networks but is not responsible for the implementation and operation of these segmented environments. | DS-12 | | 10.7.1<br>10.8<br>11.4.5 | | AC-4<br>AC-20<br>SC-7 |
| DS-12.1 | Transfer Device Methodology | Segment systems dedicated to transfer files from systems that store or process content and from the non-production network | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-12.2 | Transfer Device Methodology | Place content transfer systems in a Demilitarized Zone (DMZ) and not in the content/production network | | | | | | |
| DS-12.3 | Transfer Device Methodology | Remove content from content transfer devices immediately after successful transmission/receipt | | | | | | |
| DS-13.0 | Client Portal | Restrict access to web portals which are used for transferring content, streaming content and key distribution to authorized users | AWS provides customers the ability to create and manage a client portal. AWS does not implement or manage this portal on behalf of customers. | DS-13 | | 11.2.2<br>11.2.4<br>11.3.2<br>11.4.5<br>11.4.7<br>12.6.1 | | AC-2<br>AC-3<br>AC-4<br>AC-6<br>AC-20<br>IA-5<br>RA-3<br>RA-5<br>SC-10 |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-13.1 | Client Portal | Assign unique credentials (e.g., username and password) to portal users and distribute credentials to clients securely | | | | | | |
| DS-13.2 | Client Portal | Ensure users only have access to their own digital assets (i.e., client A must not have access to client B's content) | | | | | | |
| DS-13.3 | Client Portal | Place the web portal on a dedicated server in the DMZ and limit access to/from specific IPs and protocols | | | | | | |
| DS-13.4 | Client Portal | Prohibit the use third-party production tracking software that is hosted on internet web server unless approved by client | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-13.5 | Client Portal | Use HTTPS and enforce use of a strong cipher suite (e.g.,SSLv3 or TLS v1) for the internal/external web portal | | | | | | |
| DS-13.6 | Client Portal | Do not use persistent cookies or cookies that store credentials in plaintext | | | | | | |
| DS-13.7 | Client Portal | Set access to content on internal or external portals to expire automatically at predefined intervals, where configurable | | | | | | |
| DS-13.8 | Client Portal | Test for web application vulnerabilities annually | | | | | | |
| DS-13.9 | Client Portal | Allow only authorized personnel to request the establishment of a connection with the telecom service provider | | | | | | |

| No. | Security Topic | Best Practice | AWS Implementation | MPAA | AWS SOC | ISO 27002* | PCI | NIST 800-53* |
|---|---|---|---|---|---|---|---|---|
| DS-13.10 | Client Portal | Prohibit transmission of content using e-mail (including webmail) from the non-production network, and manage exceptions using the exception policy | | | | | | |
| DS-13.11 | Client Portal | Review access to the client web portal at least quarterly | | | | | | |

# Appendix C: AWS alignment with the Australian Signals Directorate (ASD) Cloud Computing Security Considerations

The Cloud Computing Security Considerations was created to assist agencies in performing a risk assessment of services offered by Cloud Service Providers. The following provides AWS alignment to the Security Considerations, published on September 2012. For additional details refer to:
http://www.asd.gov.au/publications/csocprotect/Cloud_Computing_Security_Considerations.pdf

| Key Area | Questions | AWS RESPONSE |
|---|---|---|
| Maintaining Availability and Business Functionality | a. Business criticality of data or functionality. Am I moving business critical data or functionality to the cloud? | AWS customers retain control and ownership of their content. Customers are responsible for the classification and use of their content. |
| | b. Vendor's business continuity and disaster recovery plan. Can I thoroughly review a copy of the vendor's business continuity and disaster recovery plan that covers the availability and restoration of both my data and the vendor's services that I use? How much time does it take for my data and the services that I use to be recovered after a disaster, and do the vendor's other customers that are larger and pay more money than me get prioritization? | AWS customers retain control and ownership of their data. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. In case of failure, automated processes move customer data traffic away from the affected area.<br><br>AWS SOC 1 Type 2 report provides further details. ISO 27001 standard Annex A, domain 11. 2 provides additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification.<br><br>Customers utilize AWS to enable faster disaster recovery of their critical IT systems without incurring the infrastructure expense of a second physical site. The AWS cloud supports many popular disaster recovery (DR) architectures from "pilot light" environments that are ready to scale up at a moment's notice to "hot standby" environments that enable rapid failover. To learn more about Disaster Recovery on AWS visit http://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf.<br><br>AWS provides customers with the capability to implement a robust continuity plan, including the utilization of frequent server instance back-ups, data redundancy replication, and multi-region/availability zone deployment architectures. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. In case of failure, automated processes move customer data traffic away from the affected area.<br><br>AWS data centers incorporate physical protection against environmental risks. AWS's physical protection against environmental risks has been validated by an independent auditor and has been certified as being in alignment with ISO 27002 best practices. Refer to ISO 27001 standard, Annex A domain 9.1 and the AWS SOC 1 Type II report for additional information. |

| Key Area | Questions | AWS RESPONSE |
|---|---|---|
| | c. My data backup plan. Will I spend additional money to maintain an up to date backup copy of my data located either at my agency's premises, or stored with a second vendor that has no common points of failure with the first vendor? | AWS customers retain control and ownership of their content and it is the customer's responsibility to manage their data backup plans<br><br>AWS allows customers to move data as needed on and off AWS storage. AWS Import/Export service for S3 accelerates moving large amounts of data into and out of AWS using portable storage devices for transport. AWS allows customers to perform their own backups to tapes using their own tape backup service provider. However, a tape backup is not a service provided by AWS. Amazon S3 service is designed to drive the likelihood of data loss to near zero percent and the durability equivalent of multi-site copies of data objects is achieved through data storage redundancy. For information on data durability and redundancy, please refer to the AWS web site.<br><br>AWS offers a range of cloud computing services to support Disaster Recovery. To learn more about Disaster Recovery on AWS visit http://media.amazonwebservices.com/AWS_Disaster_Recovery.pdf. |
| | d. My business continuity and disaster recovery plan. Will I spend additional money to replicate my data or business functionality with a second vendor that uses a different data center and ideally has no common points of failure with the first vendor? This replication should preferably be configured to automatically "failover", so that if one vendor's services become unavailable, control is automatically and smoothly transitioned to the other vendor. | Customers retain control and ownership of their data. Customers can export their AMIs and use them on premise or at another provider (subject to software licensing restrictions). Refer to the AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.<br><br>AWS allows customers to move data as needed on and off AWS storage. AWS Import/Export service for S3 accelerates moving large amounts of data into and out of AWS using portable storage devices for transport. AWS allows customers to perform their own backups to tapes using their own tape backup service provider. However, a tape backup is not a service provided by AWS.<br><br>AWS data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is "cold." In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Each Availability Zone is designed as an independent failure zone. This means that Availability Zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by Region). In addition to discrete uninterruptable power supply (UPS) and onsite backup generation facilities, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability Zones are all redundantly connected to multiple tier-1 transit providers. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones. Distributing applications across multiple Availability Zones provides the ability to remain resilient in the face of most failure modes including natural disasters or system failures.<br><br>AWS SOC 1 Type 2 report provides further details. ISO 27001 standard Annex A, domain 11. 2 provides additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification. |

| Key Area | Questions | AWS RESPONSE |
|---|---|---|
| | e. My network connectivity to the cloud. Is the network connectivity between my agency's users and the vendor's network adequate in terms of availability, traffic throughput (bandwidth), delays (latency) and packet loss? | Customers can also choose their network path to AWS facilities, including multiple VPN endpoints in each AWS Region. In addition, AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your data center, office, or colocation environment, which in many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.<br><br>Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. |
| | f. Vendor's guarantee of availability. Does the Service Level Agreement (SLA guarantee that the vendor will provide adequate system availability an quality of service,<br>using their robust system architecture and business processes? | AWS does commit to high levels of availability in its service level agreements (SLAs). For example, Amazon EC2 commits to annual uptime percentage of at least 99.95% during the service year. Amazon S3 commits to monthly uptime percentage of at least 99.99% Service credits are provided in the case these availability metrics are not met.<br><br>Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones. Distributing applications across multiple Availability Zones provides the ability to remain resilient in the face of most failure modes including natural disasters or system failures.<br><br>AWS utilizes automated monitoring systems to provide a high level of service performance and availability. Proactive monitoring is available through a variety of online tools both for internal and external use. Systems within AWS are extensively instrumented to monitor key operational metrics. Alarms are configured to notify operations and management personnel when early warning thresholds are crossed on key operational metrics. An on-call schedule is used such that personnel are always available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel.<br><br>AWS Network Management is regularly reviewed by independent third party auditors as a part of AWS ongoing compliance with SOC, PCI DSS, ISO 27001 and FedRAMP[sm]. |
| | g. Impact of outages. Can I tolerate the maximum possible downtime of the SLA? Are the scheduled outage windows acceptable both in duration and time of day, or will scheduled outages interfere with my critical business processes? | AWS does not require systems to be brought offline to perform regular maintenance and system patching. AWS's own maintenance and system patching generally do not impact customers. Maintenance of instances themselves is controlled by the customer. |
| | h. SLA inclusion of scheduled outages. Does the SLA guaranteed availability percentage include scheduled outages? | AWS does not operate an environment with scheduled outage as AWS provides customers the ability to architect their environment to take advantage of multiple Availability Zones and regions. |

| Key Area | Questions | AWS RESPONSE |
|---|---|---|
| | i. SLA compensation. Does the SLA adequately reflect the actual damage caused by a breach of the SLA such as unscheduled downtime or data loss? | AWS provides customer remuneration for losses they may incur due to outages in alignment with AWS's Service Level Agreement. |
| | j. Data integrity and availability. How does the vendor implement mechanisms such as redundancy and offsite backups to prevent corruption or loss of my data, and guarantee both the integrity and the availability of my data? | AWS data integrity controls as described in AWS SOC 1 Type II report provides reasonable assurance that data integrity is maintained through all phases including transmission, storage and processing.<br><br>In addition, refer to ISO 27001 standard, Annex A, domain 12.2 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard.<br><br>Data centers are built in clusters in various global regions. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Customers should architect their AWS usage to take advantage of multiple Regions and Availability Zones.<br><br>You choose where to store your data by specifying a region (for Amazon S3) or an availability zone within a region (for EBS). Data stored in Amazon EBS is redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge. However, Amazon EBS replication is stored within the same availability zone, not across multiple zones.<br><br>Amazon S3 provides a highly durable storage infrastructure. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 Region. Once stored, Amazon S3 maintains the durability of objects by quickly detecting and repairing any lost redundancy. Amazon S3 also regularly verifies the integrity of data stored using checksums. If corruption is detected, it is repaired using redundant data. Data stored in S3 is designed to provide 99.999999999% durability and 99.99% availability of objects over a given year.<br><br>Refer to AWS Overview of Security Processes whitepaper for additional details - available at http://aws.amazon.com/security |
| | k. Data restoration. If I accidentally delete a file, email or other data, how much time does it take for my data to be partially or fully restored from backup, and is the maximum acceptable time captured in the SLA? | AWS customers retain control and ownership of their data. AWS provides customers the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. |

| Key Area | Questions | AWS RESPONSE |
|---|---|---|
| | l. Scalability. How much available spare computing resources does the vendor provide to enable my usage of the vendor's services to scale at short notice? | The AWS cloud is distributed, highly secure and resilient, giving customers large scaling potential. Customers may scale up or down, paying for only what they use. |
| | m. Changing vendor. If I want to move my data to my agency or to a different vendor, or if the vendor suddenly becomes bankrupt or otherwise quits the cloud business, how do I get access to my data in a vendor-neutral format to avoid vendor lock-in? How cooperative will the vendor be? How do I ensure that my data is permanently deleted from the vendor's storage media? For Platform as a Service, which standards does the vendor use that facilitate portability and interoperability to easily move my application to a different vendor or to my agency? | Customers retain control and ownership of their data. Customers can export their AMIs and use them on premise or at another provider (subject to software licensing restrictions). Refer to the AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security.<br><br>AWS allows customers to move data as needed on and off AWS storage. AWS Import/Export service for S3 accelerates moving large amounts of data into and out of AWS using portable storage devices for transport. AWS allows customers to perform their own backups to tapes using their own tape backup service provider. However, a tape backup is not a service provided by AWS. |

| Key Area | Questions | AWS RESPONSE |
|---|---|---|
| Protecting Data from Unauthorized Access by a Third Party | a. Choice of cloud deployment model. Am I considering using a potentially less secure public cloud, a potentially more secure hybrid cloud or community cloud, or a potentially most secure private cloud? | AWS' Compliance and Security teams have established an information security framework and policies based on the Control Objectives for Information and related Technology (COBIT) framework. The AWS security framework integrates the ISO 27002 best practices and the PCI Data Security Standard.<br><br>Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security. AWS provides third party attestations, certifications, Service Organization Controls 1 (SOC 1) Type II report and other relevant compliance reports directly to our customers under NDA.<br><br>Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the Amazon Web Services (AWS) Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can easily customize the network configuration for your Amazon VPC. For example, you can create a public-facing subnet for your webservers that has access to the Internet, and place your backend systems such as databases or application servers in a private-facing subnet with no Internet access. You can leverage multiple layers of security, including security groups and network access control lists, to help control access to Amazon EC2 instances in each subnet.<br><br>Additionally, you can create a Hardware Virtual Private Network (VPN) connection between your corporate data center and your VPC and leverage the AWS cloud as an extension of your corporate data center |
| | b. Sensitivity of my data. Is my data to be stored or processed in the cloud classified, sensitive, private, or data that is publicly available such as information from my public web site? Does the aggregation of my data make it more sensitive than any individual piece of data? For example, the sensitivity may increase if storing a significant amount of data, or storing a variety of data that if compromised would facilitate identity theft. If there is a data compromise, could I demonstrate my due diligence to senior management, government officials and the public? | AWS customers retain control and ownership of their data and may implement a structured data-classification program to meet their requirements. |

| Key Area | Questions | AWS RESPONSE |
|---|---|---|
| | c. Legislative obligations. What obligations do I have to protect and manage my data under various legislation, for example the Privacy Act, the Archives Act, as well as other legislation specific to the type of data? Will the vendor contractually accept adhering to these obligations to help me ensure that the obligations are met to the satisfaction of the Australian Government? | AWS customers retain responsibility to ensure their usage of AWS is within compliance of applicable laws and regulations. AWS communicates its security and control environment to customers through industry certifications and third party attestations, white papers (available at http://aws.amazon.com/security) and providing certifications, reports and other relevant documentation directly to AWS customers.<br><br>AWS has published a whitepaper on using AWS in the context of Australian privacy considerations, available at http://d0.awsstatic.com/whitepapersp/compliance/Using_AWS_in_the_context_of_Australian_Privacy_Considerations.pdf |
| | d. Countries with access to my data. In which countries is my data stored, backed up and processed? Which foreign countries does my data transit? In which countries is the failover or redundant data centers? Will the vendor notify me if the answers to these questions change? | AWS customers choose the AWS Region or regions in which their content and servers will be located. This allows customers with geographic specific requirements to establish environments in a location of their choice. AWS customers in Australia can choose to deploy their AWS services exclusively in the Asia Pacific (Sydney) region and store their content onshore in Australia. If the customer makes this choice, their content will be located in Australia unless the customer chooses to move the data. Customers can replicate and back up content in more than one region, but AWS does not move or replicate customer content outside of the customer's chosen region or regions.<br><br>AWS is vigilant about customers' security and does not disclose or move data in response to a request from the Australian, U.S. or other government unless legally required to do so in order to comply with a legally valid and binding order, such as a subpoena or a court order, or as is otherwise required by applicable law. Non-U.S. governmental or regulatory bodies typically must use recognized international processes, such as Mutual Legal Assistance Treaties with the U.S. government, to obtain valid and binding orders. Additionally, our practice is to notify customers where practicable before disclosing their content so they can seek protection from disclosure, unless we are legally prevented from doing so. |

| Key Area | Questions | AWS RESPONSE |
|---|---|---|
| | e. Data encryption technologies. Are hash algorithms, encryption algorithms and key lengths deemed appropriate by the DSD ISM used to protect my data when it is in transit over a network, and stored on both the vendor's computers and on backup media? The ability to encrypt data while it is being processed by the vendor's computers is still an emerging technology and is an area of current research by industry and academia. Is the encryption deemed strong enough to protect my data for the duration of time that my data is sensitive? | AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS, SimpleDB and EC2. VPC sessions are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Customers may also use third-party encryption technologies. Internally, AWS establishes and manages cryptographic keys for required cryptography employed within the AWS infrastructure. AWS produces, controls and distributes symmetric cryptographic keys using NIST approved key management technology and processes in the AWS information system. An AWS developed secure key and credential manager is used to create, protect and distribute symmetric keys and is used to secure and distribute: AWS credentials needed on hosts, RSA public/private keys and X.509 Certifications.<br><br>AWS cryptographic processes are reviewed by independent third party auditors for our continued compliance with SOC, PCI DSS, ISO 27001 and FedRAMP[sm].<br><br>The AWS CloudHSM service allows you to protect your encryption keys within HSMs designed and validated to government standards for secure key management. You can securely generate, store, and manage the cryptographic keys used for data encryption such that they are accessible only by you. AWS CloudHSM helps you comply with strict key management requirements without sacrificing application performance.<br><br>The AWS CloudHSM service works with Amazon Virtual Private Cloud (VPC). CloudHSMs are provisioned inside your VPC with an IP address that you specify, providing simple and private network connectivity to your Amazon Elastic Compute Cloud (EC2) instances. Placing CloudHSMs near your EC2 instances decreases network latency, which can improve application performance. AWS provides dedicated and exclusive access to CloudHSMs, isolated from other AWS customers. Available in multiple Regions and Availability Zones (AZs), AWS CloudHSM allows you to add secure and durable key storage to your Amazon EC2 applications |
| | f. Media sanitization. What processes are used to sanitize the storage media storing my data at its end of life, and are the processes deemed appropriate by the DSD ISM? | When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. |

| Key Area | Questions | AWS RESPONSE |
|---|---|---|
| | g. Vendor's remote monitoring and management. Does the vendor monitor, administer or manage the computers that store or process my data? If yes, is this performed remotely from foreign countries or from Australia? Can the vendor provide patch compliance reports and other details about the security of workstations used to perform this work, and what controls prevent the vendor's employees from using untrustworthy personally owned laptops? | Moving IT infrastructure to AWS services creates a model of shared responsibility between the customer and AWS. This shared model can help relieve customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. |
| | h. My monitoring and management. Can I use my existing tools for integrity checking, compliance checking, security monitoring and network management, to obtain visibility of all my systems regardless of whether these systems are located locally or in the cloud? Do I have to learn to use additional tools provided by the vendor? Does the vendor even provide such a mechanism for me to perform monitoring? | AWS Cloudwatch provides monitoring for AWS cloud resources and the applications customers run on AWS. Refer to aws.amazon.com/cloudwatch for additional details. AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to status.aws.amazon.com<br><br>The AWS Trusted Advisor inspects your AWS environment and makes recommendations when opportunities exist to save money, improve system performance and reliability, or help close security gap. |
| | i. Data ownership. Do I retain legal ownership of my data, or does it belong to the vendor and may be considered an asset for sale by liquidators if the vendor declares bankruptcy? | AWS customers retain ownership and control of their data. AWS only uses each customer's content to provide the AWS services selected by each customer to that customer and does not use customer content for any secondary purposes. AWS treats all customer content the same and has no insight as to what type of content the customer chooses to store in AWS. AWS simply makes available the compute, storage, database and networking services selected by customer – AWS does not require access to customer content to provide its services |

| Key Area | Questions | AWS RESPONSE |
|---|---|---|
| | j. Gateway technologies. What technologies does the vendor use to create a secure gateway environment? Examples include firewalls, traffic flow filters, content filters, and antivirus software and data diodes where appropriate. | The AWS network provides significant protection against traditional network security issues and customers can implement further protection. Refer to the AWS Overview of Security whitepaper (available at http://aws.amazon.com/security) for additional details.<br><br>Amazon assets (e.g. laptops) are configured with anti-virus software that includes e-mail filtering and malware detection.<br><br>AWS Network Firewall management and Amazon's anti-virus program are reviewed by independent third party auditors as a part of AWS ongoing compliance with SOC, PCI DSS, ISO 27001 and FedRAMP$^{sm}$. |
| | k. Gateway certification. Is the vendor's gateway environment certified against government security standards and regulations? | AWS obtains certain industry certifications and independent third party attestations which include the AWS Gateway environment. |
| | l. Email content filtering. For email Software as a Service, does the vendor provide customizable email content filtering that can enforce my agency's email content policy? | A Customer can utilize a system to host e-mail capabilities, however in that case it is the Customer's responsibility to employ the appropriate levels of spam and malware protection at e-mail entry and exit points and update spam and malware definitions when new releases are made available. |

| Key Area | Questions | AWS RESPONSE |
|---|---|---|
| | m. Policies and processes supporting the vendor's IT security posture. Can I have details of how the vendor's computer and network security posture is supported by policies and processes including threat and risk assessments, ongoing vulnerability management, a change management process that incorporates security, penetration testing, logging and regular log analysis, use of security products endorsed by the Australian Government, and compliance with Australian government security standards and regulations? | Policies and procedures have been established by AWS Information Security based upon the COBIT framework, ISO 27001 standards and the PCI DSS requirements.<br><br>AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. In addition AWS publishes a SOC 1 Type II report. Refer to the SOC 1 report for further details. The AWS Risk and Compliance whitepaper for additional details - available at http://aws.amazon.com/security.<br><br>AWS customers are able to identify key controls managed by AWS. Key controls are critical to the customer's control environment and require an external attestation of the operating effectiveness of these key controls in order to comply with compliance requirements—such as the annual financial audit. For this purpose, AWS publishes a wide range of specific IT controls in its Service Organization Controls 1 (SOC 1) Type II report. The SOC 1 report, formerly the Statement on Auditing Standards (SAS) No. 70, Service Organizations report and commonly referred to as the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) report, is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). The SOC 1 audit is an in-depth audit of both the design and operating effectiveness of AWS' defined control objectives and control activities (which include control objectives and control activities over the part of the infrastructure AWS manages). "Type II" refers to the fact that each of the controls described in the report are not only evaluated for adequacy of design, but are also tested for operating effectiveness by the external auditor. Because of the independence and competence of AWS' external auditor, controls identified in the report should provide customers with a high level of confidence in AWS' control environment. |
| | n. Technologies supporting the vendor's IT security posture. Can I have details of how the vendor's computer and network security posture is supported by direct technical controls including timely application of security patches, regularly updated antivirus software, defense in depth mechanisms to protect against unknown vulnerabilities, hardened operating systems and software applications configured with the strongest possible security settings, intrusion detection and prevention systems, and data loss prevention mechanisms? | AWS provides third party attestations, certifications, Service Organization Controls 1 (SOC 1) Type II report and other relevant compliance reports directly to our customers under NDA.<br><br>AWS Security regularly scans all Internet facing service endpoint IP addresses for vulnerabilities (these scans do not include customer instances). AWS Security notifies the appropriate parties to remediate any identified vulnerabilities. In addition, external vulnerability threat assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership.<br><br>In addition, the AWS control environment is subject to regular internal and external risk assessments. AWS engages with external certifying bodies and independent auditors to review and test the AWS overall control environment. |

| Key Area | Questions | AWS RESPONSE |
|---|---|---|
| | o. Auditing the vendor's IT security posture. Can I audit the vendor' implementation of security measures, including performing scans and other penetration testing of the environment provided to me? If there is justifiable reason why auditing is not possible, which reputable third party has performed audits and other vulnerability assessments? What sort of internal audits does the vendor perform, and which compliance standards and other recommended practices from organization's such as the Cloud Security Alliance are used for these assessments? Can I thoroughly review a copy of recent resulting reports? | AWS provides third party attestations, certifications, Service Organization Controls 1 (SOC 1) Type II report and other relevant compliance reports directly to our customers under NDA.<br><br>Customers can request permission to conduct scans of their cloud infrastructure as long as they are limited to the customer's instances and do not violate the AWS Acceptable Use Policy. Advance approval for these types of scans can be initiated by submitting a request via the AWS Vulnerability / Penetration Testing Request Form.<br><br>AWS Security regularly engages independent security firms to perform external vulnerability threat assessments. The AWS SOC 1 Type 2 report provides additional details on the specific control activities executed by AWS. |
| | p. User authentication. What identity and access management systems does the vendor support for users to log in to use Software as a Service? | AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups and use permissions to allow and deny their access to AWS resources.<br><br>AWS supports identity federation that makes it easier to manage users by maintaining their identities in a single place. AWS IAM includes support for the Security Assertion Markup Language (SAML) 2.0, an open standard used by many identity providers. This new feature enables federated single sign-on, or SSO, empowering users to log into the AWS Management Console or make programmatic calls to AWS APIs, by using assertions from a SAML-compliant identity provider, such as Shibboleth and Windows Active Directory Federation Services. |
| | q. Centralized control of data. What user training, policies and technical controls prevent my agency's users from using unapproved or insecure computing devices without a trusted operating environment to store or process sensitive data accessed using Software as a Service? | N/A |

| Key Area | Questions | AWS RESPONSE |
|---|---|---|
| | r. Vendor's physical security posture. Does the vendor use physical security products and devices that are endorsed by the Australian Government? How is the vendor's physical data center designed to prevent the tampering or theft of servers, infrastructure and the data stored thereon? Is the vendor's physical data center accredited by an authoritative third party? | The definition of AWS-defined logical and physical controls is documented in the SOC 1 Type II report (SSAE 16), and the report is available for review by audit and compliance teams. AWS ISO 27001 and other certifications are also available for auditors to review.<br><br>Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. Physical access is strictly controlled both at the perimeter and at building ingress points and includes, but is not limited to, professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. Physical access points to server locations are recorded by closed circuit television camera (CCTV) as defined in the AWS Data Center Physical Security Policy. Images are retained for 90 days, unless limited to 30 days by legal or contractual obligations<br><br>AWS provides data center physical access and information to approved employees and contractors who have a legitimate business need for such privileges. All visitors are required to present identification and are signed in and escorted by authorized staff.<br><br>See the SOC 1 Type II report for specific controls related to physical access, data center access authorization, and other related controls.<br><br>Refer to ISO 27001 standard, Annex A, domain 9.1 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |
| | s. Software and hardware procurement. What procurement process is used to ensure that cloud infrastructure software and hardware has been supplied by a legitimate source and has not been maliciously modified in transit? | In alignment with ISO 27001 standards, AWS Hardware assets are assigned an owner, tracked and monitored by the AWS personnel with AWS proprietary inventory management tools. AWS procurement and supply chain team maintain relationships with all AWS suppliers.<br><br>Refer to ISO 27001 standard, Annex A, domain 7.1 for additional details. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |

| Key Area | Questions | AWS RESPONSE |
|---|---|---|
| Protecting Data from Unauthorized Access by the Vendor's Customers | a. Customer segregation. What assurance do I have that the virtualization and "multi-tenancy" mechanisms guarantee adequate logical and network segregation between multiple tenants, so that a malicious customer using the same physical computer as me cannot access my data? | Amazon EC2 currently utilizes a highly customized version of the Xen hypervisor. The hypervisor is regularly assessed for new and existing vulnerabilities and attack vectors by internal and external penetration teams, and is well suited for maintaining strong isolation between guest virtual machines. The AWS Xen hypervisor security is regularly evaluated by independent auditors during assessments and audits.<br><br>All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. Customers retain control and ownership of their data, thus it is their responsibility to choose to encrypt the data. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. VPC sessions are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security. |
| | b. Weakening my security posture. How would using the vendor's cloud infrastructure weaken my agency's existing network security posture? Would the vendor advertise me as one of their customers without my explicit consent, thereby assisting an adversary that is specifically targeting me? | AWS customers are considered confidential and would not advertise customer details without explicit consent. Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the Amazon Web Services (AWS) Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. |
| | c. Dedicated servers. Do I have some control over which physical computer runs my virtual machines? Can I pay extra to ensure that no other customer can use the same physical computer as me e.g. dedicated servers or virtual private cloud? | VPC allows customers to launch Amazon EC2 instances that are physically isolated at the host hardware level; they will run on single tenant hardware. A VPC can be created with 'dedicated' tenancy, in which case all instances launched into the VPC will utilize this feature. Alternatively, a VPC may be created with 'default' tenancy, but customers may specify 'dedicated' tenancy for particular instances launched into the VPC. |
| | d. Media sanitization. When I delete portions of my data, what processes are used to sanitize the storage media before it is made available to another customer, and are the processes deemed appropriate by the DSD ISM? | Customers retain ownership and control of their content and provide customers with the ability to delete their data.<br><br>When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. |

| Key Area | Questions | AWS RESPONSE |
|---|---|---|
| Protecting Data from Unauthorized Access by Rogue Vendor Employees | a. Data encryption key management. Does the vendor know the password or key used to decrypt my data, or do I encrypt and decrypt the data on my computer so the vendor only ever has encrypted data? | AWS Customers manage their own encryption unless they are utilizing AWS server side encryption service. In this case, AWS does create a unique encryption key per tenant. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. |
| | b. Vetting of vendor's employees. What personnel employment checks and vetting processes does the vendor perform to ensure that employees are trustworthy? | AWS conducts criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees commensurate with the employee's position and level of access to AWS facilities. |
| | c. Auditing vendor's employees. What robust identity and access management system do the vendor's employees use? What auditing process is used to log and review the actions performed by the vendor's employees? | In alignment with ISO 27001 standards, AWS has established formal policies, procedures to delineate the minimum standards for logical access to AWS resources. AWS SOC 1 Type 2 report outlines the controls in place to manage access provisioning to AWS resources.<br><br>Refer to AWS Overview of Security Processes whitepaper for additional details - available at http://aws.amazon.com/security. |
| | d. Visitors to data center. Are visitors to data centers escorted at all times, and is the name and other personal details of every visitor verified and recorded? | All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.<br>AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely |
| | e. Physical tampering by vendor's employees. Is network cabling professionally installed to Australian standards or internationally acceptable standards, to help avoid the vendor's employees from accidentally connecting cables to the wrong computers, and to help readily highlight any deliberate attempts by the vendor's employees to tamper with the cabling? | Physical security controls include but are not limited to perimeter controls such as fencing, walls, security staff, video surveillance, intrusion detection systems and other electronic means. This includes appropriate protection for network cables.<br><br>The AWS SOC 1 Type 2 report provides additional details on the specific control activities executed by AWS.<br><br>Refer to ISO 27001 standard, Annex A, domain 9.1 for further information. AWS has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. |

| Key Area | Questions | AWS RESPONSE |
|---|---|---|
| | f. Vendor's subcontractors. Do the answers to these questions apply equally to all of the vendor's subcontractors? | Provisioning contractor / vendor access is managed the same for both employees and contractors, with responsibility shared across Human Resources (HR), Corporate Operations and Service Owners. Vendors are subject to the same access requirements as employees. |
| Handling Security Incidents | a. Timely vendor support. Is the vendor readily contactable and responsive to requests for support, and is the maximum acceptable response time captured in the SLA or simply a marketing claim that the vendor will try their best?<br><br>Is the support provided locally, or from a foreign country, or from several foreign countries using an approach that follows the sun? What mechanism does the vendor use to obtain a real-time understanding of the security posture of my use of the vendor's services so that the vendor can provide support? | AWS Support is a one-on-one, fast-response support channel that is staffed 24x7x365 with experienced and technical support engineers. The service helps customers of all sizes and technical abilities to successfully utilize the products and features provided by Amazon Web Services.<br><br>All AWS Support tiers offer customers of AWS Infrastructure Services an unlimited number of support cases with pay-by-the-month pricing and no long-term contracts. The four tiers provide developers and businesses the flexibility to choose the support tiers that meet their specific needs. |
| | b. Vendor's incident response plan. Does the vendor have a security incident response plan that specifies how to detect and respond to security incidents, in a way that is similar to incident handling procedures detailed in the DSD ISM? Can I thoroughly review a copy? | The Amazon Incident Management team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Staff operators provide 24 x 7 x 365 coverage to detect incidents and to manage the impact and resolution. AWS's incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. The AWS SOC 1 Type 2 report provides details on the specific control activities executed by AWS.<br><br>The AWS Overview of Security Processes whitepaper (available at http://aws.amazon.com/security) provides additional details. |
| | c. Training of vendor's employees. What qualifications, certifications and regular information security awareness training do the vendor's employees require, to know how to use the vendor's systems in a secure manner and to identify potential security incidents? | In alignment with ISO 27001 standard, all AWS employees complete periodic Information Security training which requires an acknowledgement to complete. Compliance audits are periodically performed to validate that employees understand and follow the established policies. Refer to AWS Overview of Security Processes Whitepaper for additional details - available at http://aws.amazon.com/security. |

| Key Area | Questions | AWS RESPONSE |
|---|---|---|
| | d. Notification of security incidents. Will the vendor notify me via secure communications of security incidents that are more serious than an agreed threshold, especially in cases where the vendor might be liable? Will the vendor automatically notify law enforcement or other authorities, who may confiscate computing equipment used to store or process my data? | Notification of security incidents are handled on a case-by-case basis and as required by applicable law. Any notification is performed via secure communications |
| | e. Extent of vendor support. How much assistance will the vendor provide me with investigations if there is a security breach such as an unauthorized disclosure of my data, or if there is a need to perform legal electronic discovery of evidence? | AWS provides infrastructure and customers manage everything else, including the operating system, the network configuration and the installed applications. Customers are responsible for responding appropriately to legal procedures involving the identification, collection, processing, analysis and production of electronic documents they store or process using AWS. Upon request, AWS may work with customers who require AWS' assistance in legal proceedings. |
| | f. My access to logs. How do I obtain access to time synchronized audit logs and other logs to perform a forensic investigation, and how are the logs created and stored to be suitable evidence for a court of law? | Customers retain control of their own guest operating systems, software and applications and are responsible for developing logical monitoring of the conditions of these systems. In alignment with ISO 27001 standards, AWS information systems utilize internal system clocks synchronized via NTP (Network Time Protocol).<br><br>AWS CloudTrail provides a simple solution to log user activity that helps alleviate the burden of running a complex logging system. Refer to aws.amazon.com/cloudtrail for additional details.<br><br>AWS Cloudwatch provides monitoring for AWS cloud resources and the applications customers run on AWS. Refer to aws.amazon.com/cloudwatch for additional details. AWS also publishes our most up-to-the-minute information on service availability on the Service Health Dashboard. Refer to status.aws.amazon.com. |
| | g. Security incident compensation. How will the vendor adequately compensate me if the vendor's actions, faulty software or hardware contributed to a security breach? | AWS's incident response program, plans and procedures have been developed in alignment with ISO 27001 standard. The AWS SOC 1 Type 2 report provides details on the specific control activities executed by AWS.<br><br>The AWS Overview of Security Processes whitepaper (available at http://aws.amazon.com/security) provides additional details. |

| Key Area | Questions | AWS RESPONSE |
|---|---|---|
| | h. Data spills. If data that I consider is too sensitive to be stored in the cloud is accidentally placed into the cloud, referred to as a data spill, how can the spilled data be deleted using forensic sanitization techniques? Is the relevant portion of physical storage media zeroed whenever data is deleted? If not, how long does it take for deleted data to be overwritten by customers as part of normal operation, noting that clouds typically have significant spare unused storage capacity? Can the spilled data be forensically deleted from the vendor's backup media? Where else is the spilled data stored, and can it be forensically deleted? | Customers retain ownership and control of their content. All data stored by AWS on behalf of customers has strong tenant isolation security and control capabilities. AWS allows customers to use their own encryption mechanisms for nearly all the services, including S3, EBS and EC2. IPSec tunnels to VPC are also encrypted. Amazon S3 also offers Server Side Encryption as an option for customers. Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security.<br><br>Refer to AWS Risk and Compliance Whitepaper for additional details - available at http://aws.amazon.com/security. |

# Appendix D: Glossary of Terms

**Authentication:** Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be.

**Availability Zone:** Amazon EC2 locations are composed of regions and Availability Zones. Availability Zones are distinct locations that are engineered to be insulated from failures in other Availability Zones and provide inexpensive, low latency network connectivity to other Availability Zones in the same region.

**DSS:** The Payment Card Industry Data Security Standard (DSS) is a worldwide information security standard assembled and managed by the Payment Card Industry Security Standards Council.

**EBS:** Amazon Elastic Block Store (EBS) provides block level storage volumes for use with Amazon EC2 instances. Amazon EBS volumes are off-instance storage that persists independently from the life of an instance.

**FedRAMP[sm]:** The Federal Risk and Authorization Management Program (FedRAMP[sm]) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP[sm] is mandatory for Federal Agency cloud deployments and service models at the low and moderate risk impact levels.

**FISMA:** The Federal Information Security Management Act of 2002. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

**FIPS 140-2:** The Federal Information Processing Standard (FIPS) Publication 140-2 is a US government security standard that specifies the security requirements for cryptographic modules protecting sensitive information.

**GLBA:** The Gramm–Leach–Bliley Act (GLB or GLBA), also known as the Financial Services Modernization Act of 1999, sets forth requirements for financial institutions with regard to, among other things, the disclosure of nonpublic customer information and the protection of threats in security and data integrity.

**HIPAA:** The Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The Administration Simplification provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the U.S. health care system.

**Hypervisor:** A hypervisor, also called Virtual Machine Monitor (VMM), is software/hardware platform virtualization software that allows multiple operating systems to run on a host computer concurrently.

**IAM:** AWS Identity and Access Management (IAM) enables a customer to create multiple Users and manage the permissions for each of these Users within their AWS Account.

**ITAR:** International Traffic in Arms Regulations (ITAR) is a set of United States government regulations that control the export and import of defense-related articles and services on the United States Munitions List (USML). Government agencies and contractors must comply with ITAR and restrict access to protected data.

**ISAE 3402:** The International Standards for Assurance Engagements No. 3402 (ISAE 3402) is the international standard on assurance engagements. It was put forth by the International Auditing and Assurance Standards Board (IAASB), a standard-setting board within the International Federation of Accountants (IFAC). ISAE 3402 is now the new globally recognized standard for assurance reporting on service organizations.

**ISO 9001:** AWS's ISO 9001 certification directly supports customers who develop, migrate and operate their quality-controlled IT systems in the AWS cloud. Customers can leverage AWS's compliance reports as evidence for their own ISO 9001 programs and industry-specific quality programs, such as GxP in life sciences, ISO 13485 in medical devices, AS9100 in aerospace, and ISO/TS 16949 in automotive. AWS customers who don't have quality system requirements will still benefit from the additional assurance and transparency that an ISO 9001 certification provides.

**ISO 27001:** ISO/IEC 27001 is an Information Security Management System (ISMS) standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO 27001 formally specifies a management system that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organizations that claim to have adopted ISO/IEC 27001 can therefore be audited and certified compliant with the standard.

**NIST:** National Institute of Standards and Technology. This agency sets detailed security standards as needed by industry or government programs. Compliance with FISMA requires agencies to adhere to NIST standards.

**Object:** The fundamental entities stored in Amazon S3. Objects consist of object data and metadata. The data portion is opaque to Amazon S3. The metadata is a set of name-value pairs that describe the object. These include some default metadata such as the date last modified and standard HTTP metadata such as Content-Type. The developer can also specify custom metadata at the time the Object is stored.

**PCI:** Refers to the Payment Card Industry Security Standards Council, an independent council originally formed by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, with the goal of managing the ongoing evolution of the Payment Card Industry Data Security Standard.

**QSA:** The Payment Card Industry (PCI) Qualified Security Assessor (QSA) designation is conferred by the PCI Security Standards Council to those individuals that meet specific qualification requirements and are authorized to perform PCI compliance assessments.

**SAS 70:** Statement on Auditing Standards No. 70: Service Organizations is an auditing statement issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). SAS 70 provides guidance to service auditors when assessing the internal controls of a service organization (such as AWS) and issuing a service auditor's report. SAS 70 also provides guidance to auditors of financial statements of an entity that uses one or more service organizations. The SAS 70 report has been replaced by the Service Organization Controls 1 report.

**Service:** Software or computing ability provided across a network (e.g., EC2, S3, VPC, etc.).

**Service Level Agreement (SLA):** A service level agreement is a part of a service contract where the level of service is formally defined. The SLA is used to refer to the contracted delivery time (of the service) or performance.

**SOC 1:** Service Organization Controls 1 (SOC 1) Type II report, formerly the Statement on Auditing Standards (SAS) No. 70, Service Organizations report (commonly referred to as the SSAE 16 report), is a widely recognized auditing standard

developed by the American Institute of Certified Public Accountants (AICPA). The international standard is referenced as the International Standards for Assurance Engagements No. 3402 (ISAE 3402).

**SSAE 16:** The Statement on Standards for Attestation Engagements No. 16 (SSAE 16) is an attestation standard published by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). The standard addresses engagements undertaken by a service auditor for reporting on controls at organizations that provide services to user entities, for which a service organization's controls are likely to be relevant to a user entities internal control over financial reporting (ICFR). SSAE 16 effectively replaces Statement on Auditing Standards No. 70 (SAS 70) for service auditor's reporting periods ending on or after June 15, 2011.

**SOC 2:** Service Organization Controls 2 (SOC 2) reports are intended to meet the needs of a broad range of users that need to understand internal control at a service organization as it relates to security, availability, processing integrity, confidentiality and privacy. These reports are performed using the AICPA Guide: Reporting on Controls at a Service Organizations Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy and are intended for use by stakeholders (e.g., customers, regulators, business partners, suppliers, directors) of the service organization that have a thorough understanding of the service organization and its internal controls.

**SOC 3**: Service Organization Controls 3 (SOC 3) reports are designed to meet the needs of uses who want assurance on the controls at a service organization related to security, availability, processing integrity, confidentiality, or privacy but do not have the need for or the knowledge necessary to make effective use of a SOC 2 Report. These reports are prepared using the AICPA/Canadian Institute of Chartered Accountants (CICA) Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy. Because they are general use reports, SOC 3 Reports can be freely distributed or posted on a website as a seal.

**Virtual Instance:** Once an AMI has been launched, the resulting running system is referred to as an instance. All instances based on the same AMI start out identical and any information on them is lost when the instances are terminated or fail.

***Version History***

**Dec 2014**

- Updates to certifications and third-party attestations summaries

**Nov 2013 version**

- Edits to IPsec tunnel encryption verbiage

**Jun 2013 version**

- Updates to certifications and third-party attestations summaries
- Updates to Appendix C: Glossary of Terms
- Minor changes to formatting

**Jan 2013 version**

- Edits to certifications and third-party attestations summaries
- Addition of the AWS Alignment with MPAA Content Security Model (Appendix B)

**Nov 2012 version**

- Edits to content and updated certification scope
- Added reference to the SOC 2 and MPAA

**Jul 2012 version**

- Edits to content and updated certification scope
- Addition of the CSA Consensus Assessments Initiative Questionnaire (Appendix A)

**Jan 2012 version**

- Minor edits to content based on updated certification scope
- Minor grammatical edits

**Dec 2011 version**

- Change to Certifications and Third-party Attestation section to reflect SOC 1/SSAE 16, FISMA Moderate, International Traffic in Arms Regulations, and FIPS 140-2
- Addition of S3 Server Side Encryption
- Added additional cloud computing issue topics

**May 2011 version**

- Initial release

***Notices***